

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073414

(43)Date of publication of application : 18.03.1997

(51)Int.Cl. G06F 12/14  
G09C 1/00  
G11B 20/10  
G11B 20/12  
G11B 20/18

(21)Application number : 08-098949

(71)Applicant : SONY CORP

(22)Date of filing : 19.04.1996

(72)Inventor : SAKO YOICHIRO  
KAWASHIMA ISAO  
KURIHARA AKIRA  
OSAWA YOSHITOMO  
OWA HIDEO

(30)Priority

Priority number : 07166698  
07187967

Priority date : 30.06.1995  
30.06.1995

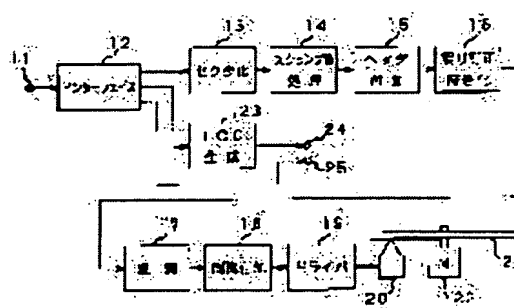
Priority country : JP  
JP

(54) METHOD AND DEVICE FOR DATA RECORDING, DATA RECORDING MEDIUM, AND METHOD AND DEVICE FOR DATA REPRODUCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To cipher data so that it is difficult to decipher the data by using simple constitution.

SOLUTION: An input is ciphered and outputted by at least one circuit among a sectoring circuit 13 which is used to process the input data into a recording signal, a scrambling processing circuit 14, a header adding circuit 15, an error correcting and encoding circuit 16, a modulating circuit 16, a modulating circuit 18, and a synchronism adding circuit 18. In this case, not only the key of the ciphering process itself in the circuit, but also which circuit has performed the ciphering process become a ciphering key.



## LEGAL STATUS

[Date of request for examination] 19.07.2001

[Date of sending the examiner's decision of rejection] 13.09.2005

[Kind of final disposal of application other than

the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision 2005-19837  
of rejection]

[Date of requesting appeal against examiner's 13.10.2005  
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-73414

(43)公開日 平成9年(1997)3月18日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 D
G 1 1 B 20/10		7736-5 D	G 1 1 B 20/10	H
	1 0 2	9295-5 D	20/12	1 0 2
	5 7 0	9558-5 D	20/18	5 7 0 N
審査請求 未請求 請求項の数33 O L (全 28 頁)				

(21)出願番号 特願平8-98949

(22)出願日 平成8年(1996)4月19日

(31)優先権主張番号 特願平7-166698

(32)優先日 平7(1995)6月30日

(33)優先権主張国 日本 (J P)

(31)優先権主張番号 特願平7-187967

(32)優先日 平7(1995)6月30日

(33)優先権主張国 日本 (J P)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 佐古 曜一郎

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 川嶋 功

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 栗原 章

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 弁理士 小池 晃 (外2名)

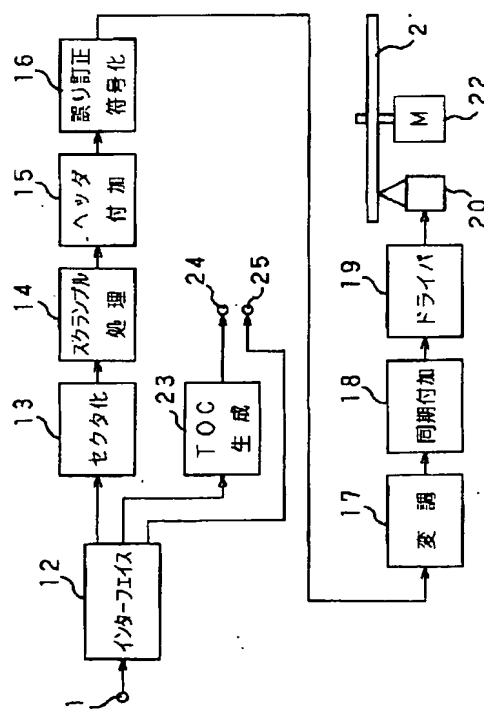
最終頁に続く

(54)【発明の名称】 データ記録方法及び装置、データ記録媒体、並びにデータ再生方法及び装置

(57)【要約】

【課題】 簡単な構成で、解読が困難な暗号化を施す。

【解決手段】 入力データを処理して記録信号とするために用いられるセクタ化回路13、スクランブル処理回路14、ヘッダ付加回路15、誤り訂正符号化回路16、変調回路18、及び同期付加回路18の内、いずれか少なくとも1つの回路で、入力に対して暗号化処理を施して出力する。回路内での暗号化処理自体の鍵のみならず、どの回路で暗号化処理を行ったかも暗号化の鍵となる。



**【特許請求の範囲】**

【請求項 1】 入力デジタルデータを所定データ量単位でセクタ化するセクタ化工程と、このセクタ化されたデジタルデータにヘッダを付加するヘッダ付加工程と、このヘッダ付加されたデジタルデータに誤り訂正符号を付加する誤り訂正符号化工程と、この誤り訂正符号化されたデジタルデータを所定の変調方式で変調する変調工程と、この変調されたデジタル信号に同期パターンを付加する同期付加工程と、この同期パターンが付加されたデジタル信号を記録媒体に記録する記録工程とを有し、上記セクタ化工程、ヘッダ付加工程、誤り訂正符号化工程、変調工程、及び同期付加工程のいずれか少なくとも 1 つの工程について、入力に対して暗号化処理を施して出力することを特徴とするデータ記録方法。

【請求項 2】 上記セクタ化工程でセクタ化されたデジタルデータ又は上記ヘッダ付加工程でヘッダが付加されたデジタルデータに対して、同一パターンを除去するためのランダム化処理を施すスクランブル処理工程を設け、

上記セクタ化工程、ヘッダ付加工程、誤り訂正符号化工程、変調工程、同期付加工程、及びスクランブル処理工程のいずれか少なくとも 1 つの工程について、入力に対して暗号化処理を施して出力することを特徴とする請求項 1 記載のデータ記録方法。

【請求項 3】 上記暗号化処理に用いられる鍵情報を複数設定しておき、これらの鍵情報を所定タイミングで切り換えることを特徴とする請求項 1 記載のデータ記録方法。

【請求項 4】 上記セクタ化工程、ヘッダ付加工程、誤り訂正符号化工程、変調工程、及び同期付加工程のいずれの工程で暗号化処理が施されたかを鍵情報とすることを特徴とする請求項 1 記載のデータ記録方法。

【請求項 5】 上記誤り訂正符号化工程の誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すことを特徴とする請求項 1 記載のデータ記録方法。

【請求項 6】 上記誤り訂正符号は積符号であることを特徴とする請求項 1 記載のデータ記録方法。

【請求項 7】 入力デジタルデータを所定データ量単位でセクタ化するセクタ化手段と、このセクタ化手段から出力されたデジタルデータにヘッダを付加するヘッダ付加手段と、このヘッダ付加手段から出力されたデジタルデータに誤り訂正符号を付加する誤り訂正符号化手段と、この誤り訂正符号化手段から出力されたデジタルデータを所定の變調方式で變調する變調手段と、この變調手段から出力されたデジタル信号に同期パタ

ーンを付加する同期付加手段と、

この同期付加手段から出力されたデジタル信号を記録媒体に記録する記録手段とを有し、

上記セクタ化手段、ヘッダ付加手段、誤り訂正符号化手段、變調手段、及び同期付加手段のいずれか少なくとも 1 つの手段は、入力に対して暗号化処理を施して出力することを特徴とするデータ記録装置。

【請求項 8】 上記セクタ化手段でセクタ化されたデジタルデータ又は上記ヘッダ付加手段でヘッダが付加されたデジタルデータに対して、同一パターンを除去するためのランダム化処理を施すスクランブル処理手段を設け、

上記セクタ化手段、ヘッダ付加手段、誤り訂正符号化手段、變調手段、同期付加手段、及びスクランブル処理手段のいずれか少なくとも 1 つの手段は、入力に対して暗号化処理を施して出力することを特徴とする請求項 7 記載のデータ記録装置。

【請求項 9】 上記誤り訂正符号化手段は、誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すデータ変換手段を有することを特徴とする請求項 7 記載のデータ記録装置。

【請求項 10】 入力デジタルデータが所定データ量単位でセクタ化され、ヘッダが付加され、誤り訂正符号化され、所定の變調方式で變調され、同期パターンが付加されると共に、これらのセクタ化、ヘッダ付加、誤り訂正符号化、變調、及び同期付加のいずれかの際に、入力に対して暗号化処理が施された信号が記録されて成ることを特徴とするデータ記録媒体。

【請求項 11】 データ記録媒体から読み取られたデジタル信号から同期信号を分離する同期分離工程と、この同期分離されたデジタル信号に対して所定の變調方式に従った復調を施す復調工程と、

この復調されて得られたデジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化工程と、

この誤り訂正復号化処理されたデジタルデータを所定のセクタに分解するセクタ分解工程と、

このセクタ分解されたデジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離工程とを有し、

上記同期分離工程、復調工程、誤り訂正復号化工程、セクタ分解工程、及びヘッダ分離工程の内、いずれか少なくとも 1 つの工程に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の工程について、入力に対して暗号の復号化処理を施して出力することを特徴とするデータ再生方法。

【請求項 12】 上記セクタ分解工程でセクタに分解されたデジタルデータ又は上記ヘッダ分離工程でヘッダが分離されたデジタルデータに対して、記録時のスクランブルを解くデスクランブル処理工程を設け、

上記同期分離工程、復調工程、誤り訂正復号化工程、セクタ分解工程、ヘッダ分離工程、及びデスクランブル処理工程の内、いずれかが少なくとも1つの工程に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の工程について、入力に対して暗号の復号化処理を施して出力することを特徴とする請求項1記載のデータ再生方法。

【請求項13】 記録媒体から読み取られたデジタル信号から同期信号を分離する同期分離手段と、この同期分離手段から出力されたデジタル信号に対して所定の変調方式に従った復調を施す復調手段と、この復調手段から得られたデジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化手段と、この誤り訂正復号化手段から出力されたデジタルデータを所定のセクタに分解するセクタ分解手段と、このセクタ分解手段から出力されたデジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離手段とを有し、

上記同期分離手段、復調手段、誤り訂正復号化手段、セクタ分解手段、及びヘッダ分離手段の内、いずれかが少なくとも1つの手段に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の手段にて、入力に対して暗号の復号化処理を施して出力することを特徴とするデータ再生装置。

【請求項14】 上記セクタ分解手段から出力されたデジタルデータ又は上記ヘッダ分離手段から出力されたデジタルデータに対して、記録時のスクランブルを解くデスクランブル処理を施すデスクランブル処理手段を設け、

上記同期分離手段、復調手段、誤り訂正復号化手段、セクタ分解手段、ヘッダ分離手段、及びデスクランブル処理手段の内、いずれかが少なくとも1つの手段に対応する記録時の手段について暗号化処理が施されており、この記録時に暗号化処理が施された手段に対応する再生時の手段について、入力に対して暗号の復号化処理を施して出力することを特徴とする請求項13記載のデータ再生装置。

【請求項15】 入力デジタルデータに誤り訂正符号化処理を施して記録媒体に記録するデータ記録方法において、

上記誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すことを特徴とするデータ記録方法。

【請求項16】 上記データ変換は、データと上記鍵情報との論理演算、鍵情報を用いた置換、転置、あるいは関数演算の少なくとも1つにより行われることを特徴とする請求項15記載のデータ記録方法。

【請求項17】 上記データ変換を施すデータの個数を

暗号化の難易度に応じて変化させることを特徴とする請求項15記載のデータ記録方法。

【請求項18】 入力デジタルデータに誤り訂正符号化処理を施して記録媒体に記録するデータ記録装置において、

暗号化の鍵情報の入力手段と、

この入力手段からの鍵情報に応じて、上記誤り訂正符号化処理の際に取り扱われるデータの少なくとも一部に対してデータ変換を施す手段とを有することを特徴とするデータ記録装置。

【請求項19】 入力デジタルデータに誤り訂正符号化処理を施す際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換が施されて得られた信号が記録されて成ることを特徴とするデータ記録媒体。

【請求項20】 誤り訂正符号化処理が施されて記録媒体に記録された信号を再生するデータ再生方法において、

上記誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換が施されており、

上記誤り訂正符号化処理に対応する誤り訂正復号化処理の際に取り扱われるデータの内の上記暗号化の鍵情報に応じたデータに上記データ変換に対する逆変換を施すことを特徴とするデータ再生方法。

【請求項21】 誤り訂正符号化処理が施されて記録媒体に記録された信号を再生するデータ再生装置において、

上記誤り訂正符号化処理の際に取り扱われるデータの内のデータ変換が施されたデータを示す暗号化の鍵情報を入力する鍵情報入力手段と、

上記誤り訂正符号化処理に対応する誤り訂正復号化処理を行うと共に、上記鍵情報入力手段からの暗号化の鍵情報に応じたデータに上記データ変換に対する逆変換を施す誤り訂正復号化手段とを有することを特徴とするデータ再生装置。

【請求項22】 入力データに対して記録のための信号処理を施して記録媒体の所定のデータ記録領域に記録するデータ記録方法において、

所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部として上記記録媒体のデータ記録領域とは別の領域に書き込まれた情報を用いることを特徴とするデータ記録方法。

【請求項23】 上記鍵情報として、媒体固有の識別情報、記録装置固有の識別情報、媒体製造装置固有の識別情報、製造者／販売者の識別情報、地域情報、外部から供給される識別情報、の少なくとも1つを用いることを特徴とする請求項12記載のデータ記録方法。

【請求項24】 入力データに対して記録のための信号処理を施して記録媒体の所定のデータ記録領域に記録す

るデータ記録装置において、所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部として上記記録媒体のデータ記録領域とは別の領域に書き込まれた情報を用いることを特徴とするデータ記録装置。

【請求項 2 5】 データ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて暗号化処理が施されたデータが上記データ記録領域に書き込まれて成ることを特徴とするデータ記録媒体。

【請求項 2 6】 データ記録媒体のデータ記録領域から読み取られ、記録時に暗号化処理の施されたデジタル信号に対して再生のための信号処理を施す際に、上記データ記録媒体の上記データ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて、暗号復号化処理を施すことを特徴とするデータ再生方法。

【請求項 2 7】 上記鍵情報として、媒体固有の識別情報、記録装置固有の識別情報、媒体製造装置固有の識別情報、製造者／販売者の識別情報、再生装置固有の識別情報、地域情報、外部から供給される識別情報、の少なくとも 1 つを用いることを特徴とする請求項 2 6 記載のデータ再生方法。

【請求項 2 8】 データ記録媒体のデータ記録領域から読み取られ、記録時に暗号化処理の施されたデジタル信号に対して再生のための信号処理を施すデータ再生装置であって、上記データ記録媒体の上記データ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて、暗号復号化処理を施すことを特徴とするデータ再生装置。

【請求項 2 9】 入力デジタルデータを所定データ量単位でセクタ化するセクタ化工程と、このセクタ化されたデジタルデータに対してスクランブル処理を施すスクランブル処理工程と、このスクランブル処理されたデジタルデータにヘッダを付加するヘッダ付加工程と、このヘッダ付加されたデジタルデータに誤り訂正符号を付加する誤り訂正符号化工程と、この誤り訂正符号化されたデジタルデータを所定の変調方式で変調する変調工程と、この変調されたデジタル信号に同期パターンを付加する同期付加工程と、この同期パターンが付加されたデジタル信号を記録媒体に記録する記録工程とを有し、上記スクランブル処理工程の初期値及び生成多項式の少なくとも一方を暗号化の鍵情報に応じて変化させることを特徴とするデータ記録方法。

【請求項 3 0】 入力デジタルデータを所定データ量単位でセクタ化するセクタ化手段と、このセクタ化手段から出力されたデジタルデータに対

して、初期値及び生成多項式の少なくとも一方が暗号化の鍵情報に応じて変化するスクランブル処理を施すスクランブル処理手段と、

このスクランブル処理手段から出力されたデジタルデータにヘッダを付加するヘッダ付加手段と、

このヘッダ付加手段から出力されたデジタルデータに誤り訂正符号を付加する誤り訂正符号化手段と、

この誤り訂正符号化手段から出力されたデジタルデータを所定の変調方式で変調する変調手段と、

この変調手段から出力されたデジタル信号に同期パターンを付加する同期付加手段と、

この同期付加手段から出力されたデジタル信号を記録媒体に記録する記録手段とを有することを特徴とするデータ記録装置。

【請求項 3 1】 入力デジタルデータが所定データ量単位でセクタ化され、初期値及び生成多項式の少なくとも一方が暗号化の鍵情報に応じて変化させられたスクランブル処理が施され、ヘッダが付加され、誤り訂正符号化され、所定の変調方式で変調された信号が記録されて成ることを特徴とするデータ記録媒体。

【請求項 3 2】 データ記録媒体から読み取られたデジタル信号から同期信号を分離する同期分離工程と、この同期分離されたデジタル信号に対して所定の変調方式に従った復調を施す復調工程と、

この復調されて得られたデジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化工程と、

この誤り訂正復号化処理されたデジタルデータを所定のセクタに分解するセクタ分解工程と、

このセクタ分解されたデジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離工程と、

このヘッダ分離されたデジタルデータに対して記録時の暗号化の鍵情報により初期値及び生成多項式の少なくとも一方を変化させてスクランブルを解くデスクランブル処理を施すデスクランブル処理工程とを有することを特徴とするデータ再生方法。

【請求項 3 3】 記録媒体から読み取られたデジタル信号から同期信号を分離する同期分離手段と、

この同期分離手段から出力されたデジタル信号に対して所定の変調方式に従った復調を施す復調手段と、

この復調手段から得られたデジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化手段と、

この誤り訂正復号化手段から出力されたデジタルデータを所定のセクタに分解するセクタ分解手段と、

このセクタ分解手段から出力されたデジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離手段と、

このヘッダ分離手段から出力されたデジタルデータに対して記録時の暗号化の鍵情報により初期値及び生成多項式の少なくとも一方を変化させてスクランブルを解くデスクランブル処理を施すデスクランブル処理手段とを有することを特徴とするデータ再生装置。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、コピー防止や不正使用の阻止、あるいは課金システムに適用可能なデータ記録方法及び装置、データ記録媒体、並びにデータ再生方法及び装置に関する。

**【0002】**

【従来の技術】近年において、光ディスク等のデジタル記録媒体の大容量化と普及により、コピー防止や不正使用の阻止が重要とされてきている。すなわち、デジタルオーディオデータやデジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる被害が生じてきているのが実情である。

**【0003】**

【発明が解決しようとする課題】ところで、デジタルオーディオデータやデジタルビデオデータの不法コピー等を回避するためには、いわゆるSCMS（シリアルコピー管理システム）やCGMS（コピー世代管理システム）の規格が知られているが、これは記録データの特定部分にコピー禁止フラグを立てるようなものであるため、デジタル2値信号の丸ごとコピーであるいわゆるダンプコピー等の方法によりデータを抜き出される問題がある。

【0004】また、例えば特開昭60-116030号公報に開示されているように、コンピュータデータの場合には、ファイル内容自体を暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。これは、情報流通の形態として、情報が暗号化されて記録されたデジタル記録媒体を配布しておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものであるが、簡単で有用な暗号化の手法の確立が望まれている。

【0005】本発明は、上述したような実情に鑑みてなされたものであり、簡単な構成で暗号化が行え、データの暗号化によりコピー防止や不正使用の防止が簡単な仕組みで実現でき、暗号の解読が困難であり、また、暗号の難易度あるいは深度の制御も容易に行えるようなデータ記録方法及び装置、データ記録媒体、並びにデータ再生方法及び装置の提供を目的とする。

**【0006】**

【課題を解決するための手段】上記の課題を解決するために、本発明に係るデータ記録方法は、入力デジタルデータを所定データ量単位でセクタ化するセクタ化工程と、ヘッダを付加するヘッダ付加工程と、誤り訂正符号化工程と、所定の変調方式で変調する変調工程と、同期パターンを付加する同期付加工程との、いずれか少なく

とも1つの工程について、入力に対して暗号化処理を施して出力することを特徴とすることにより、上述の課題を解決する。これらの暗号化処理が施され得る工程の1つに、同一パターンを除去するためのランダム化処理を施すスクランブル処理工程を含めてもよい。

【0007】このデータ記録方法をデータ記録装置に適用することができる。

【0008】上記データ記録方法で得られた信号が記録されたデータ記録媒体を提供することができる。

【0009】本発明に係るデータ再生方法は、上記データ記録方法で記録されたデータ記録媒体を再生する際に、同期分離工程、復調工程、誤り訂正復号化工程、セクタ分解工程、及びヘッダ分離工程の内、いずれか少なくとも1つの工程に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の工程について、入力に対して暗号の復号化処理を施すことにより、上述の課題を解決する。これらの暗号復号化処理が施され得る工程の1つに、記録時のスクランブルを解くデスクランブル処理を施すスクランブル処理工程を含めてもよい。

【0010】このデータ再生方法をデータ再生装置に適用することができる。

【0011】また、本発明に係るデータ記録方法は、誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すことを特徴としている。このデータ変換としては、データと上記鍵情報との論理演算や、転置、置換等を挙げることができる。

【0012】また、本発明に係るデータ記録方法は、所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部として記録媒体のデータ記録領域とは別の領域に書き込まれた情報を用いることにより、上述の課題を解決する。これをデータ記録装置、データ記録媒体に適用することができる。

【0013】また、本発明に係るデータ再生方法は、記録時に暗号化処理の施されたデジタル信号に対して再生のための信号処理を施す際に、データ記録媒体のデータ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて、暗号復号化処理を施すことにより、上述の課題を解決する。これをデータ再生装置に適用することができる。

【0014】さらに、本発明に係るデータ記録方法は、スクランブル処理工程の初期値及び生成多項式の少なくとも一方を暗号化の鍵情報に応じて変化させることにより、上述の課題を解決する。

【0015】また、本発明に係るデータ再生方法は、記録時の暗号化の鍵情報により初期値及び生成多項式の少なくとも一方を変化させてスクランブルを解くデスクランブル処理を施すことにより、上述の課題を解決する。

【0016】入力デジタルデータを所定データ量単位でセクタ化し、ヘッダを付加し、誤り訂正符号化処理を施し、所定の変調方式で変調し、同期パターンを付加して、記録媒体に記録する。これらの工程のいずれか少なくとも1つの工程について、入力に対して暗号化処理を施して出力することにより、どの工程で暗号化処理が施されたかも暗号の鍵となり、暗号の難易度が高くなる。

【0017】暗号化の鍵情報の少なくとも一部を、記録媒体のデータ記録領域とは別の領域に書き込んでおき、再生時にこの鍵情報の少なくとも一部の情報を読み取って、暗号復号化に用いる。暗号復号化の鍵情報が、記録媒体のデータ記録領域内の情報のみで完結しないため、暗号化の難易度が高まる。

【0018】データ列の同一パターンを除去するためのランダム化を主目的とするスクランブル処理の際に、生成多項式及び初期値の少なくとも一方を、暗号化の鍵に応じて変化させる。既存のスクランブル処理を暗号化に流用できる。

【0019】

【発明の実施の形態】以下、本発明に係るいくつかの好ましい実施の形態について、図面を参照しながら説明する。

【0020】図1は、本発明の第1の実施の形態を概略的に示すブロック図である。この図1において、入力端子11には、例えばアナログのオーディオ信号やビデオ信号をデジタル変換して得られたデータやコンピュータデータ等のデジタルデータが供給されている。この入力デジタルデータは、インターフェース回路12を介して、セクタ化回路13に送られ、所定データ量単位、例えば2048バイト単位でセクタ化される。セクタ化されたデータは、スクランブル処理回路14に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路15に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路16に送られる。誤り訂正符号化回路16では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路17では、所定の変調方式に従って、例えば8ビットデータを16チャンネルビットの変調データに変換し、同期付加回路18に送る。同期付加回路18では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ19を介して記録ヘッド20に送っている。記録ヘッド20は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体21に上記変調された

記録信号の記録を行う。このディスク状記録媒体21は、スピンドルモータ22により回転駆動される。

【0021】なお、上記スクランブル処理回路14は、必須ではなく、また、ヘッダ付加回路15の後段に挿入して、ヘッダ付加されたデジタルデータに対してスクランブル処理を施して誤り訂正符号化回路16に送るようにしてもよい。

【0022】ここで、セクタ化回路13、スクランブル処理回路14、ヘッダ付加回路15、誤り訂正符号化回路16、変調回路17、及び同期付加回路18のいずれか少なくとも1つの回路は、入力に対して暗号化処理を施して出力するような構成を有している。好ましくは、2つ以上の回路で暗号化処理を施すことが挙げられる。この暗号化処理の鍵情報は、記録媒体21のデータ記録領域とは別の領域に書き込まれた識別情報、例えば媒体固有の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、国別コード等の地域情報、外部から供給される識別情報等を少なくとも一部に用いている。このように、媒体のデータ記録領域以外に書き込まれる識別情報は、例えば上記インターフェース回路12からTOC

(Table of contents) 生成回路23を介して端子24に送られる情報であり、また、インターフェース回路12から直接的に端子25に送られる情報である。これらの端子24、25からの識別情報が、暗号化の際の鍵情報の一部として用いられ、回路13～18の少なくとも1つ、好ましくは2以上で、この鍵情報を用いた入力データに対する暗号化処理が施される。

【0023】この場合、回路13～18のどの回路において暗号化処理が施されたかも選択肢の1つとなっており、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、1つの回路で暗号化処理が施されていれば、6つの選択肢の1つを選ぶことが必要となり、2つの回路で暗号化処理が施されていれば、2つの回路の組み合わせの数に相当する15個の選択肢の内から1つを選ぶことが必要となる。6つの回路13～18の内の1～6つの回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、十分に暗号の役割を果たすものである。

【0024】また、暗号化の鍵情報を所定タイミング、例えばセクタ周期で切り換えることが挙げられる。この所定タイミングで鍵情報の切り換える場合に、切り換えを行うか否かや、切換周期、複数の鍵情報の切換順序等の情報も鍵として用いることができ、暗号化のレベルあるいは暗号の難易度、解き難さ、解読の困難さをさらに高めることができる。

【0025】次に、各回路13～18の構成及び暗号化処理の具体例について説明する。



【0026】先ず、セクタ化回路13においては、例えば図2に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図2において、上記図1のインターフェース回路12からの出力を、2出力の切換スイッチ31に送り、この切換スイッチ31の一方の出力を偶奇インターリーブ33を介してセクタ化器34に送り、切換スイッチ31の他方の出力をそのままセクタ化器34に送っている。セクタ化器34では、例えば入力データの2048バイト単位でまとめて1セクタとしている。このセクタ化回路13の切換スイッチ32の切換動作を、鍵となる1ビットの制御信号で制御するわけである。偶奇インターリーブ33は、図3のAに示すような偶数バイト36aと奇数バイト36bとが交互に配置された入力データの1セクタ分を、図3のBに示すように、偶数データ部37aと奇数データ部37bとに分配して出力する。さらに、図3のCに示すように、1セクタ内の所定の領域39を鍵情報により特定し、この領域39内のデータについてのみ偶数データ部39aと奇数データ部39bとに分配するようにしてもよい。この場合には、領域39の特定の仕方を複数通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。

【0027】次に、スクランブル処理回路14には、例えば図4に示すように、15ビットのシフトレジスタを用いたいわゆるパラレルブロック同期タイプのスクランブラを用いることができる。このスクランブラのデータ入力用の端子35には、LSB（最下位ビット）が時間的に先となる順序、いわゆるLSBファーストで、上記セクタ化回路13からのデータが入力される。スクランブル用の15ビットのシフトレジスタ14aは、排他的論理和（ExOR）回路14bを用いて生成多項式 $x^{15} + x + 1$ に従ったフィードバックがかけられ、15ビットのシフトレジスタ14aには、図5に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図5のプリセット値の選択番号は、例えばセクタアドレスの下位側4ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ14aからの出力データと端子35からの入力データとは、ExOR回路14cにより排他的論理和がとられて、端子14dより取り出され、図1のヘッダ付加回路15に送られる。

【0028】ここで、上記生成多項式及びプリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記生成多項式を変化させるには、例えば図6に示すような構成を用いればよい。この図6において、15ビットのシフトレジスタ14aの各ビットからの出力が切換スイッチ14fの各被選択端子に送られ、この切換スイッチ14fは制御端子14gからの例えば4ビットの制御データに

よって切換制御され、切換スイッチ14fからの出力はExOR回路14bに送られている。このような構成の制御端子14gの制御データを変化させることにより、生成多項式 $x^{15} + x^n + 1$ のnを変化させることができる。また、上記プリセット値を変化させるには、上記図5のプリセット値テーブルの各プリセット値を、例えば16バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND）、論理和（OR）、シフト演算等を使用できる。なお、生成多項式を変化させるための構成は図6の構成に限定されず、シフトレジスタの段数や取り出すタップ数を任意に変更してもよい。

【0029】次に、ヘッダ付加回路15について説明する。先ず、図7はセクタフォーマットの具体例を示しており、1セクタは、2048バイトのユーザデータ領域41に対して、4バイトの同期領域42と、16バイトのヘッダ領域43と、4バイトの誤り検出符号（E D C）領域44とが付加されて構成されている。誤り検出符号領域44の誤り検出符号は、ユーザデータ領域41及びヘッダ領域43に対して生成される32ビットのCRC符号から成っている。ヘッダ付加回路15での暗号化処理としては、同期いわゆるデータシンクに対して、ヘッダのアドレス及びCRCに対して施すことが挙げられる。

【0030】セクタの同期すなわちデータシンクに対して暗号化処理を施す一例としては、4バイトの同期領域42の各バイトに割り当てられたバイトパターンを、図8の「A」、「B」、「C」、「D」にてそれぞれ表すとき、2ビットの鍵情報を用いて、この4バイトの内容をバイト単位でシフトあるいはローテートすることが挙げられる。すなわち、2ビットの鍵が「0」のとき「A B C D」、「1」のとき「B C D A」、「2」のとき「C D A B」、「3」のとき「D A B C」のように切り換えることにより、この鍵が合致しないとセクタの同期がとれなくなり、正常な再生が行えない。なお、上記バイトパターン「A」～「D」としては、例えばISO 646のキャラクタコード等を使用できる。

【0031】ヘッダ領域43内には、図9に示すように、いわゆる巡回符号であるCRC 45、コピーの許可／不許可やコピー世代管理等のためのコピー情報46、多層ディスクのどの層かを示す層47、アドレス48、予備49の各領域が設けられている。この内で、アドレス48の32ビットにビットスクランブル、この場合には、ビット単位での転置処理を施すことにより、暗号化

が行える。また、CRC45の生成多項式として、 $x^{16} + x^{15} + x^2 + 1$  が用いられている場合、第2、第3項の $x^{15}$ 、 $x^2$ の代わりに、 $x^{15} \sim x$ に対応する15ビットを鍵に応じて変化させることが挙げられる。また、CRC45の16ビットと鍵情報とを論理演算することも挙げられる。

【0032】なお、上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダ、あるいは媒体製造装置の固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【0033】次に、誤り訂正符号化回路16の具体例を図10、図11に示す。これらの図10、図11において、入力端子51には、上記図1のヘッダ付加回路15からのデータが第1の符号化器であるC1エンコーダ52に供給されている。この具体例においては、誤り訂正符号化の1フレームは148バイトあるいは148シンボルのデータから成るものとしており、入力端子51からのデジタルデータが148バイト毎にまとめられて、第1の符号化器であるC1エンコーダ52に供給される。C1エンコーダ52では8バイトのPパリティが付加され、インターリーブのための遅延回路53を介して第2の符号化器であるC2エンコーダ54に送られる。C2エンコーダ54では14バイトのQパリティが付加され、このQパリティは遅延回路55を介してC1エンコーダ52に帰還されている。このC1エンコーダ52からのP、Qパリティを含む170バイトが取り出されて、遅延回路56を介し、インバータ部57aを有する再配列回路57を介して出力端子58より取り出され、図1の変調回路17に送られる。

【0034】このような誤り訂正符号化回路において暗号化処理を施す場合には、例えば再配列回路57内のインバータ部57aの各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、22バイトのP、Qパリティに対して再配列回路57のインバータ部57aのインバータによる反転が行われて出力されるが、これらのインバータのいくつかを無くしたり、C1データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられる。

【0035】このようなデータ変換を施す場合、基準構成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばC1エンコーダについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが9であるため、最大4バイトまでのエラー検出訂正が行え、消失（イレ

ジャ）ポインタがあれば最大8バイトまでの訂正が可能であることから、違いが5箇所以上あると、C1符号では常に訂正不可又は誤訂正となる。違いが4箇所の場合は、他に1バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが3、2、1箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【0036】この場合、予めインバータの変更を行う場所を例えば2箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を2箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【0037】さらに、インバータの挿入あるいは変更位置としては、図10、図11の再配列回路57内の位置に限定されず、例えばC1エンコーダ52の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、上記データ変換としては、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしたり、データを暗号化の鍵情報に応じて転置するようにしたり、データを暗号化の鍵情報に応じて置換するようにしてもよい。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【0038】ここで、図12は、上記誤り訂正符号化回路16の他の具体例として、再配列回路57内のインバータ部57aの後段の位置に排他的論理和（ExOR）回路群61を挿入し、C1エンコーダ52の前段すなわち入力側の位置にもExOR回路群66を挿入した例を示している。

【0039】具体的に、ExOR回路群61は、C1エンコーダ52から遅延回路56、及び上記再配列回路57のインバータ部57aを介して取り出される170バイトのデータ、すなわち情報データ $C1_{170n+169} \sim C1_{170n+22}$ 及びパリティデータ $P1_{170n+21} \sim P1_{170n+14}$ 、 $Q1_{170n+13} \sim Q1_{170n}$ のデータに対して排他的論理和（ExOR）回路を用いたデータ変換を行い、ExOR回路群66は、148バイトの入力データ $B_{148n} \sim B_{148n+147}$ に対して排他的論理和（ExOR）回路を用いたデータ変換を行う。これらのExOR回路群61、66に用いられるExOR回路は、1バイトすなわち8ビットの入力データと1ビットの制御データで指示される所定の8ビットデータとの排他的論理和（ExOR）をそれぞれとるような8ビットExOR回路であり、このような8ビットExOR回路（所定の8ビットデータがオール1の場合はインバー

タ回路に相当する)が、ExOR回路群 61 では 170 個、ExOR回路群 66 では 148 個用いられている。

【0040】この図 12 においては、170 ビットの鍵情報が端子 62 に供給され、いわゆる D ラッチ回路 63 を介して ExOR 回路群 61 内の 170 個の各 ExOR 回路にそれぞれ供給されている。D ラッチ回路 63 は、イネーブル端子 64 に供給された 1 ビットの暗号化制御信号に応じて、端子 62 からの 170 ビットの鍵情報をそのまま ExOR 回路群 61 に送るか、オールゼロ、すなわち 170 ビットの全てを“0”とするかが切換制御される。ExOR 回路群 61 の 170 個の各 ExOR 回路の内、D ラッチ回路 63 から“0”が送られた ExOR 回路は、再配列回路 57 内のインバータ部 57a からのデータをそのまま出力し、D ラッチ回路 63 から“1”が送られた ExOR 回路は、再配列回路 57 内のインバータ部 57a からのデータを反転して出力する。オールゼロのときには、再配列回路 57 内のインバータ部 57a からのデータをそのまま出力することになる。また、ExOR 回路群 66 については、148 個の ExOR 回路を有し、鍵情報が 148 ビットであること以外は、上記 ExOR 回路群 61 の場合と同様であり、端子 67 に供給された 148 ビットの鍵情報が D ラッチ回路 68 を介して ExOR 回路群 66 内の 148 個の ExOR 回路にそれぞれ送られると共に、D ラッチ回路 68 はイネーブル端子 69 の暗号化制御信号により 148 ビットの鍵情報がオールゼロかが切換制御される。

【0041】この図 12 の例において、ExOR 回路群 61 は、C1 エンコーダ 52 から遅延回路 56、インバータ部 57a を介して取り出される 170 バイトのデータとしての情報データ  $C1_{170n+169} \sim C1_{170n+22}$  及びパリティデータ  $P1_{170n+21} \sim P1_{170n+14}$ 、 $Q1_{170n+13} \sim Q1_{170n}$  のデータに対して排他的論理和 (ExOR) 回路を用いたデータ変換を行っているが、パリティデータについてはデータ変換を行わず、残り 148 バイトの情報データ  $C1_{170n+169} \sim C1_{170n+22}$  に対して、148 ビットの鍵情報に応じたデータ変換を行わせるようにしてもよい。

【0042】この図 12 の回路においても、上記図 10、図 11 の場合と同様な作用効果が得られることは勿論である。また、ExOR 回路群 61、66 のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【0043】上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダあるいは媒体製造装置の固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【0044】なお、上記データ変換手段としての ExOR 回路群 61、66 の代わりに、AND、OR、NAND、

NOR、インバート回路群等を使用してもよい。また、8 ビット単位で 1 ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、8 ビットの情報データに対して 8 ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの 1 ワードに相当する 8 ビットの内の各ビットに対してそれぞれ AND、OR、ExOR、NAND、NOR、インバート回路を組み合わせ使用してもよい。この場合には、例えば 148 バイトすなわち  $148 \times 8$  ビットのデータに対して、 $148 \times 8$  ビットの鍵データが用いられることになり、さらに AND、OR、ExOR、NAND、NOR、インバート回路を組み合わせ使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせ使用することも可能である。

【0045】さらに、この第 1 の実施の形態においては、クロスインターリーブ型の誤り訂正符号の例について説明したが、積符号の場合にも同様に適用可能であり、これについては本発明の第 2 の実施の形態として後述する。

【0046】次に、図 1 の変調回路 17 での暗号化処理について、図 13 を参照しながら説明する。この図 13 において、入力端子 71 には、上記誤り訂正符号化回路 16 からのデータが 8 ビット (1 バイト) 毎に供給され、入力端子 72 には 8 ビットの鍵情報が供給されており、これらの 8 ビットデータは、論理演算回路の一例としての ExOR 回路 73 に送られて排他的論理和がとられる。この ExOR 回路 73 からの 8 ビット出力が、所定の変調方式の変調器、例えば 8-16 変換回路 74 に送られて、16 チャンネルビットに変換される。この 8-16 変換回路 74 での 8-16 変調方式の一例としてはいわゆる EFM プラス変調方式が挙げられる。

【0047】この図 13 の例では、データ変調の前に 8 ビットの鍵情報を用いた暗号化処理を施しているが、鍵情報のビット数は 8 ビットに限定されず、また、8-16 変調の際の変換テーブルの入出力の対応関係を鍵情報に応じて変化させるようにしてもよい。鍵情報には、上述した媒体固有の識別情報等を使用できることは勿論である。

【0048】次に、同期付加回路 18 について説明する。同期付加回路 18 では、例えば図 14 に示すような 4 種類の同期ワード S0~S3 を用いて、上記 8-16 変調のフレーム単位で同期をとっている。この 8-16 変調フレーム (例えば EFM プラスフレーム) は、例えば 85 データシンボルである 1360 チャンネルビットから成り、この 1 フレーム 1360 チャンネルビット毎

に 32 チャンネルビットの同期ワードが付加されると共に、このフレームを上記 C1 符号や C2 符号に対応させて構造化し、C1 符号系列の先頭フレームの同期ワードと他のフレームの同期ワードを異ならせる等して、上記 4 種類の同期ワード S0～S3 を使い分けている。これらの同期ワード S0～S3 は、直前のワードの“1”、“0”の状態やいわゆるデジタルサムあるいは直流値等に依じてそれぞれ 2 つの同期パターン a、b を有している。

【0049】このような 4 種類の同期ワード S0～S3 の選択を、例えば図 15 に示すような回路を用いて、2 ビットの鍵情報 75 に依じて変更することにより、暗号化が行える。すなわち、上記 4 種類の同期ワード S0～S3 を指定する 2 ビットデータ 76 の各ビットと、上記 2 ビットの鍵情報 75 の各ビットとが、2 つの ExOR 回路 77、78 によりそれぞれ排他的論理和され、新たな同期ワード指定データ 79 となる。これにより、上記フレーム構造における同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が変更され、暗号化がなされることになる。

【0050】なお、同期ワードの種類数をさらに増やしてそれらの内から 4 種類の同期ワードを取り出す取り出し方を暗号化の鍵により決定するようにしてもよい。この鍵情報としては、上述した媒体固有の識別情報等が使用できる。

【0051】次に図 16 は、記録媒体の一例としての光ディスク等のディスク状記録媒体 101 を示している。このディスク状記録媒体 101 は、中央にセンタ孔 102 を有しており、このディスク状記録媒体 101 の内周から外周に向かって、プログラム管理領域である TOC (table of contents) 領域となるリードイン (lead in) 領域 103 と、プログラムデータが記録されたプログラム領域 104 と、プログラム終了領域、いわゆるリードアウト (lead out) 領域 105 とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域 104 にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域 103 で管理される。

【0052】上記鍵情報の一部として、データ記録領域であるプログラム領域 104 以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、TOC 領域であるリードイン領域 103 や、リードアウト領域 105 に、識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにすると共に、これを鍵情報として、上述した 6 つの回路 13～18 の少なくとも 1 つ、好ましくは 2 つ以上で暗号化処理を施して得られた信号をデータ記録領域であるプログラム領域 104 に記録するよ

うにする。再生時には、上記識別情報を、暗号を復号するための鍵情報として用いるようにすればよい。また、リードイン領域 103 よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。

【0053】次に、本発明のデータ再生方法、データ再生装置の実施の形態について、図 17 を参照しながら説明する。

【0054】図 17 において、記録媒体の一例としてのディスク状記録媒体 101 は、スピンドルモータ 108 により回転駆動され、光学ピックアップ装置等の再生ヘッド装置 109 により媒体記録内容が読み取られる。

【0055】再生ヘッド装置 109 により読み取られたデジタル信号は、TOC デコーダ 111 及びアンプ 112 に送られる。TOC デコーダ 111 からは、ディスク状記録媒体 101 の上記リードイン領域 103 に TOC 情報の一部として記録された上記識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報が読み取られ、この識別情報が暗号を復号化するための鍵情報の少なくとも一部として用いられる。この他、再生装置内部の CPU 122 から、再生装置固有の識別情報や、外部からの識別情報を出力するようにし、この識別情報を鍵情報の少なくとも一部として用いるようにしてもよい。なお、外部からの識別情報としては、通信回線や伝送路等を介して受信された識別情報や、いわゆる IC カード、ROM カード、磁気カード、光カード等を読み取って得られた識別情報等が挙げられる。

【0056】再生ヘッド装置 109 からアンプ 112 を介し、PLL (位相ロックループ) 回路 113 を介して取り出されたデジタル信号は、同期分離回路 114 に送られて、上記図 1 の同期付加回路 18 で付加された同期信号の分離が行われる。同期分離回路 114 からのデジタル信号は、復調回路 115 に送られて、上記図 1 の変調回路 17 の変調を復調する処理が行われる。具体的には、16 チャンネルビットを 8 ビットのデータに変換するような処理である。復調回路 115 からのデジタルデータは、誤り訂正復号化回路 116 に送られて、図 1 の誤り訂正符号化回路 16 での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路 117 によりセクタに分解され、ヘッダ分離回路 118 により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路 117 及びヘッダ分離回路 118 は、上記図 1 のセクタ化回路 13 及びヘッダ付加回路 15 に対応するものである。次に、デスクランブル処理回路 119 により、上記図 1 のスクランブル処理回路 14 におけるスクランブル処理の逆処理としてのデスクランブル処

理が施され、インターフェース回路 120 を介して出力端子 121 より再生データが取り出される。

【0057】ここで、上述したように、記録時には、上記図 1 のセクタ化回路 13、スクランブル処理回路 14、ヘッダ付加回路 15、誤り訂正符号化回路 16、変調回路 17、及び同期付加回路 18 のいずれか少なくとも 1 つの回路において暗号化処理が施されており、この暗号化処理が施された回路に対応する再生側の回路 114～119 にて、暗号を復号化する処理が必要とされる。すなわち、上記図 1 のセクタ化回路 13 にて暗号化処理が施されている場合には、セクタ分解回路 117 にて暗号化の際の鍵情報を用いた暗号の復号化処理が必要とされる。以下同様に、図 1 のスクランブル処理回路 14 での暗号化処理に対応してデスクランブル処理回路 119 での暗号復号化処理が、図 1 のヘッダ付加回路 15 での暗号化処理に対応してヘッダ分離回路 118 での暗号復号化処理が、図 1 の誤り訂正符号化回路 16 での暗号化処理に対応して誤り訂正復号化回路 116 での暗号復号化処理が、図 1 の変調回路 17 での暗号化処理に対応して復調回路 115 での暗号復号化処理が、さらに図 1 の同期付加回路 18 での暗号化処理に対応して同期分離回路 114 での暗号復号化処理が、それぞれ必要とされる。

【0058】同期分離回路 114 での暗号復号化処理は、上記図 14 や図 15 と共に説明したように、複数種類、例えば 4 種類の同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が鍵情報に応じて変更され、暗号化がなされたものを、鍵情報に応じて検出することで行われる。

【0059】次に、復調回路 115 での暗号復号化処理は、図 18 に示すように、同期分離回路 114 から 16-8 変換回路 131 に送られて 16 チャンネルビットが 8 ビットデータに変換されたものを、上記図 13 の ExOR 回路 73 に対応する ExOR 回路 132 に送り、端子 133 からの 8 ビットの鍵情報との排他的論理和をとることで、図 13 の入力端子 71 に供給された 8 ビットデータに相当するデータが復元され、これが誤り訂正復号化回路 116 に送られる。

【0060】次に、誤り訂正復号化回路 116 では、例えば上記図 10、図 11 の誤り訂正符号化処理の逆処理が、図 19、図 20 の構成により行われる。

【0061】これらの図 19、図 20 において、上記復調回路 115 にて復調されたデータの 170 バイトあるいは 170 シンボルを 1 まとまりとして、インバータ部 142a を有する再配列回路 142 を介し、遅延回路 143 を介して第 1 の復号器である C1 デコーダ 144 に送られている。この C1 デコーダ 144 に供給される 170 バイトのデータの内 22 バイトが P、Q パリティであり、C1 デコーダ 144 では、これらのパリティデータを用いた誤り訂正復号化が施される。C1 デコーダ 1

44 からは、170 バイトのデータが出力されて、遅延回路 145 を介して第 2 の復号器である C2 デコーダ 146 に送られ、パリティデータを用いた誤り訂正復号化が施される。C2 デコーダ 146 からの出力データは、図 19 の遅延・C1 デコード回路 140 に送られる。これは、上記遅延回路 143 及び C1 デコーダ 144 と同様のものであり、これらの遅延回路 143 及び C1 デコーダ 144 と同様の処理を繰り返し行うことにより誤り訂正復号化を行うものである。図 8 の例では、遅延回路 147 及び第 3 の復号器である C3 デコーダ 148 で表している。この遅延回路 147 及び C3 デコーダ 148、あるいは遅延・C1 デコード回路 140 で最終的な誤り訂正復号化が施され、パリティ無しの 148 バイトのデータが出力端子 149 を介して取り出される。この 148 バイトのデータは、上記図 10、図 11 の C1 エンコーダ 52 に入力される 148 バイトのデータに相当するものである。

【0062】そして、図 10、図 11 の誤り訂正符号化回路の再配列回路 57 内のインバータ部 57a で、インバータの有無による暗号化が施されている場合には、図 19、図 20 の誤り訂正復号化回路の再配列回路 142 内のインバータ部 142a にて、対応する暗号復号化を行うことが必要とされる。その他、図 10、図 11 と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【0063】ここで、図 21 は、上記図 12 の誤り訂正符号化回路の具体的構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【0064】この図 21 において、上記図 12 の再配列回路 57 内のインバータ部 57a の出力側に挿入された ExOR 回路群 61 に対応して、再配列回路 142 のインバータ部 142a の入力側及び遅延回路 143 の入力側の位置に、ExOR 回路群 151 が挿入され、図 12 の C1 エンコーダ 52 の入力側に挿入された ExOR 回路群 66 に対応して、C3 デコーダ 148 の出力側に ExOR 回路群 156 が挿入されている。

【0065】これらの ExOR 回路群 151、156 は、上述したように、図 12 の ExOR 回路群 61、66 によるデータ変換をそれぞれ復号化するためのデータ変換を施すものであり、ExOR 回路群 151 は、例えば 170 個の 8 ビット ExOR 回路により、また ExOR 回路群 156 は、148 個の 8 ビット ExOR 回路によりそれぞれ構成されている。なお、記録側の図 12 の誤り訂正符号化回路の ExOR 回路群 61 で、パリティデータを除く 148 バイトの情報データに対して鍵情報に応じたデータ変換が施されている場合には、ExOR 回路群 151 は 148 個の 8 ビット ExOR 回路により構成されることは勿論である。

【0066】この図 21 の端子 152 には、図 12 の端子 62 に供給される鍵情報に相当する 170 ビットの鍵

情報が供給され、いわゆる D ラッチ回路 153 を介して ExOR 回路群 151 内の 170 個の各 ExOR 回路にそれぞれ供給されている。D ラッチ回路 153 は、イネーブル端子 154 に供給された 1 ビットの暗号化制御信号に応じて、端子 152 からの 170 ビットの鍵情報をそのまま ExOR 回路群 151 に送るか、オールゼロ、すなわち 170 ビットの全てを“0”とするかが切換制御される。また、ExOR 回路群 156 については、148 個の ExOR 回路を有し、鍵情報が図 12 の端子 67 に供給される鍵情報と同様の 148 ビットであること以外は、上記 ExOR 回路群 151 の場合と同様であり、端子 157 に供給された 148 ビットの鍵情報が D ラッチ回路 158 を介して ExOR 回路群 156 内の 148 個の ExOR 回路にそれぞれ送られると共に、D ラッチ回路 158 はイネーブル端子 159 の暗号化制御信号により 148 ビットの鍵情報がオールゼロとするかが切換制御される。

【0067】このように、誤り訂正回路のインバータや ExOR 回路等を暗号化の鍵として使うことにより、簡易で大きな暗号化が実現できる。また、このインバータ等の数を制御することにより、通常でも再生不可能な暗号化レベルのデータとか、エラー状態が悪くなると再生不可能となるデータとか、セキュリティレベルの要求に応じて対応できる。すなわち、インバータや ExOR 回路等の個数をコントロールすることにより、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、また、エラー訂正のみでは回復不可能な再生不可能状態を形成することもできる。また、暗号化の鍵としては、上記図示の例のように 1 箇所当たり百数十ビットもの大きなビット数となり、鍵のビット数の大きな暗号化ができるため、データセキュリティが向上する。しかも、このようなエラー訂正符号化回路やエラー訂正復号化回路を、いわゆる LSI や IC チップのハードウェア内で実現することにより、一般ユーザからはアクセスが困難であり、この点でもデータセキュリティが高いものとなっている。

【0068】次に、セクタ分解回路 117 においては、上記図 2、図 3 と共に説明したように、記録時に上記セクタ化回路 13 で偶数・奇数バイトのインターリーブによる暗号化が施されている場合に、この偶奇インターリーブを解くような逆の処理、いわゆるデインターリーブ処理を施すものである。

【0069】また、ヘッダ分離回路 118 においては、記録時に、上記ヘッダ付加回路 15 において、上記図 7～図 9 と共に説明したような暗号化処理、すなわちセクタ同期となるデータシンクのバイトパターンの転置や、アドレス、CRC の変更がなされている場合に、これを復元するような暗号復号化処理を施すものである。

【0070】次に、図 22 は、デスクランブル処理回路 119 の具体例を示しており、端子 161 には、図 17 のヘッダ分離回路 118 からのデジタルデータが供給

されている。この端子 161 からのデジタルデータは、例えば上記図 4 に示すような構成を有するスクランブラ 163 でデスクランブル処理され、出力端子 164 より取り出される。このスクランブラ 163 についての、上記図 4 と共に説明したような生成多項式 165 及びプリセット値（あるいは初期値）166 を、認証機構 171 からの暗号の鍵情報に応じて変化させることにより、暗号復号化を行うことができる。この認証機構 171 では、上記ヘッダ情報 167 のコピー情報 46 の内容や、媒体固有のあるいは再生装置固有の固有識別情報 172 や、製造者、販売者等の共通識別情報 173 や、外部から与えられる外部識別情報 174 等により、暗号の鍵情報を生成し、この鍵情報に応じて生成多項式 165 やプリセット値 166 を制御する。

【0071】これらの各回路 114～119 のいずれで暗号復号化処理が必要とされるかの情報も、暗号の鍵情報となることは前述した通りである。また、暗号の鍵情報を所定周期、例えばセクタ周期で切り換えることができ、この切換を行うか否かや、切換周期等も鍵とすることにより、暗号化の難易度が高められる。

【0072】以上説明したように、製造者識別情報、販売者識別情報、装置識別情報等と、別途設定されるコピープロテクト情報、課金情報を組み合わせて、データを暗号化して記録しておくことにより、コピー防止、海賊盤防止、不正使用の防止等を物理フォーマットレベルで実現し得るようにしている。また、データセキュリティ機能の情報、例えばコピーの許可／不許可情報、有償／無償情報を、記録媒体及び記録／再生システムの物理フォーマットにインプリメントしている。

【0073】すなわち、セキュリティ／課金情報を予め媒体に記録しておき、媒体に記録又は未記録の識別情報を用いて、それをデータの暗号化と組み合わせることにより、簡単な仕組みでコピー防止、不正使用防止が実現できるようになる。また、物理フォーマットにそれを内在させることにより、解読が困難になる。また、ダンプコピーされても暗号化されたままであるので安全である。さらに、セクタ単位やファイル単位、ゾーン単位、レイヤ単位等で可変にできる。またさらに、通信や IC カードやリモコン等で鍵がコントロールできる。さらに、海賊盤に対して履歴が残せる。

【0074】次に、本発明の第 2 の実施の形態について説明する。この第 2 の実施の形態は、上述した第 1 の実施の形態の構成を部分的に変更したものであり、全体の基本構成は、前述した図 1 に示す通りである。この図 1 の構成の各回路 13～18 の内の変更部分について以下説明する。

【0075】図 1 のセクタ化回路 13 は前述した第 1 の実施の形態と同様に構成すればよいが、スクランブル処理回路 14 については、図 23 に示す構成を用いている。

【0076】この図23に示すスクランブル処理回路14において、データ入力用の端子35には、LSB（最下位ビット）が時間的に先となる順序、いわゆるLSBファーストで、図1のセクタ化回路13からのデータが入力される。スクランブル用の15ビットのシフトレジスタ14aは、排他的論理和（ExOR）回路14bを用いて生成多項式  $x^{15} + x^4 + 1$  に従ったフィードバックがかけられ、15ビットのシフトレジスタ14aには、図24に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図24のプリセット値の選択番号は、例えばセクタアドレスの下位側4ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ14aからの出力データと端子35からの入力データとは、ExOR回路14cにより排他的論理和がとられて、端子14dより取り出され、図1のヘッダ付加回路15に送られる。

【0077】ここで、上記プリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記図24のプリセット値テーブルの各プリセット値を、例えば16バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND）、論理和（OR）、シフト演算等を使用できる。

【0078】次に、この第2の実施の形態のセクタフォーマットとしては、例えば、図25に示すようなものを用いている。

【0079】この図25に示すように、1セクタは、1行172バイトの12行、すなわち2064バイトから成り、この中にメインデータ2048バイトを含んでいる。12行の最初の行の先頭位置には、4バイトのID（識別データ）と、2バイトのIED（IDエラー検出符号）と、6バイトのRSV（予備）とがこの順に配置されており、最後の行の終端位置には、4バイトのEDC（エラー検出符号）が配置されている。

【0080】上記ID（識別データ）の4バイトは、図26に示すように、MSB側の最初のバイト（ビットb31～b24）はセクタ情報から成り、残りの3バイト（ビットb23～b0）はセクタ番号から成っている。セクタ情報は、MSB側から順に、1ビットのセクタフォーマットタイプ、1ビットのトラッキング方法、1ビットの反射率、1ビットの予備、2ビットのエリアタイプ、2ビットの層番号の各情報から成っている。

【0081】図1のヘッダ付加回路15では、このようなセクタフォーマットにおいて、例えば上記ID（識別

データ）の内のセクタ番号の24ビットに対して、上記鍵情報に応じて例えばビット単位でのスクランブル処理である転置処理を施すことにより、暗号化を施すことができる。また、上記2バイトのIED（IDエラー検出符号）の生成多項式や、4バイトのEDC（エラー検出符号）の生成多項式等を上記鍵情報に応じて変更することによっても、あるいはこれらの情報と鍵情報とを論理演算することによっても、暗号化を施すことができる。

【0082】次に、図1の誤り訂正符号化回路16としては、図27に示すような構成の回路が用いられる。この符号化は、図28に示すような積符号あるいはブロック符号が用いられる。図27において、入力端子210には、前記図1のヘッダ付加回路15からのデータが供給され、この入力データは、第1の符号化器であるPOエンコーダ211に送られる。このPOエンコーダ211への入力データは、図28に示すように、 $B_{0,0} \sim B_{191,171}$ の172バイト×192行のデータであり、POエンコーダ211では、172列の各列192バイトのデータに対して、それぞれ16バイトずつのリード・ソロモン（RS）符号としてのRS（208,192,17）の外符号（PO）を付加している。POエンコーダ211からの出力データは、前述したような暗号化のためのデータ変換回路212を介して、インターリーブ回路213に送られてインターリーブ処理され、PIエンコーダ214に送られる。このPIエンコーダ214では、図28に示すように、上記POパリティが付加された172バイト×208行のデータの各行の172バイトのデータに対して、それぞれ10バイトずつのRS（182,172,11）の内符号（PI）を付加している。従って、このPIエンコーダ214からは、182バイト×208行のデータが出力されることになる。この出力データは、前述したような暗号化のためのデータ変換回路215を介して、出力端子216より取り出される。

【0083】ここで、データ変換回路212については、POエンコーダ211が各列毎の192バイトの入力データに対して16バイトのPOパリティを付加して208バイトのデータを出力することから、この16バイトのパリティに対して、あるいは208バイトのデータ全体に対して、前述したようなデータ変換を行うことにより暗号化を施すことができる。このデータ変換は、前述したように、端子218を介して入力される鍵情報に応じて施すようにしてもよい。また、データ変換回路215については、PIエンコーダ214が各行の172バイトのデータに対して、それぞれ10バイトずつのPIパリティを付加して182バイトのデータを出力することから、この10バイトのパリティに対して、あるいは182バイトのデータ全体に対してデータ変換を行うことにより暗号化を施すことができる。このデータ変換も、前述したように、端子219を介して入力される鍵情報に応じて施すようにしてもよい。



【0084】上記データ変換は、具体的には、前記図10、図11、図12と共に説明したように、インバータを所定位置に配設したり、ExOR回路群により鍵情報に応じて選択的にデータを反転させたり、その他、AND、OR、NAND、NOR 回路群等を使用してもよい。また、8ビット単位で1ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、8ビットの情報データに対して8ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの1ワードに相当する8ビットの内の各ビットに対してそれぞれAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用してもよい。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。また、AND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【0085】誤り訂正符号化された上記182バイト×208行のデータは、行についてインターリーブされ、13行ずつ16のグループに分けられて、各グループが記録セクタに対応付けられる。1セクタは、182バイト×13行の2366バイトとなるが、これらが変調されて、図29に示すように1行当たり2つの同期コードSYが付加される。変調には、前述した第1の実施の形態と同様に8-16変換が用いられるが、1行は2つのシンクフレームに分けられ、1シンクフレームは、32チャンネルビットの同期コードSYと1456チャンネルビットのデータ部とから成っている。図29は、変調され同期付加されて得られた1セクタ分の構造を示し、この図29に示す1セクタ分の38688チャンネルビットは、変調前の2418バイトに相当する。

【0086】図29の変調出力信号には、8種類の同期コードSY0～SY7が用いられており、これらの同期コードSY0～SY7は、上記8-16変換の状態(ステート)に応じて、ステート1及び2のときが図30の(a)、ステート3及び4のときが図30の(b)の同期パターンとなっている。

【0087】このような8種類の同期コードSY0～SY7の選択を、例えば図31に示すような回路を用いて、3ビットの鍵情報に応じて変更することにより、暗号化が行える。すなわち、上記8種類の同期コードSY0～SY7を指定する3ビットデータ221の各ビットと、上記3ビットの鍵情報222の各ビットとを、3つのExOR回路223、224、225によりそれぞれ排他

的論理和をとることにより、新たな同期コード指定データ226とする。これにより、上記フレーム構造における同期コードの使い方あるいはフレーム構造内での各種同期コードの使用位置が変更され、暗号化がなされることになる。勿論、その3ビットに対して鍵情報に応じてデータを転置したり、置換したり、シフトレジスタにより変換したりできる。また、これは関数変換でもかまわない。

【0088】次に、上述した本発明の第2の実施の形態の記録側の構成に対して、再生側の基本構成は、前記図17と同様であり、上記第2の実施の形態に示した各部の変更箇所に対応して変更された逆処理がそれぞれ施される。例えば、上記図27に示す誤り訂正符号化に対する逆処理は、図32のような構成の誤り訂正復号化回路により実現できる。

【0089】すなわち、この図32において、入力端子230には前記図17の復調回路115からの出力信号であり、上記図27の出力端子216からの出力に相当する上記図28の積符号の182バイト×208行のデータが供給されている。この入力端子230からのデータは、データ逆変換回路231に送られて、上記図27のデータ変換回路215の逆処理が行われる。データ逆変換回路231からの出力データは、PI(内符号)デコーダ232に送られて、上記図27のPIエンコーダ214の逆処理としての復号化処理すなわちPI符号を用いた誤り訂正処理が施され、上記図28の172バイト×208行のデータとなる。PIデコーダ232からの出力データは、デインターリーブ回路233で上記インターリーブ回路213での逆処理が施され、データ逆変換回路234に送られて上記図27のデータ変換回路212の逆処理が行われた後、PO(外符号)デコーダ235に送られる。POデコーダ235では、上記図27のPOエンコーダ211の逆処理としての復号化処理すなわちPO符号を用いた誤り訂正処理が施され、図28の元の172バイト×192行のデータが出力端子236を介して取り出される。上記図27のデータ変換回路212、215でのデータ変換の際に鍵情報を用いる場合には、各端子218、219にそれぞれ供給した鍵情報を、図32のデータ逆変換回路234、231の各端子239、238にそれぞれ供給して、これらの鍵情報に応じてデータ逆変換を行わせればよい。

【0090】以上説明した本発明の第2の実施の形態における効果も、前述した第1の実施の形態の場合と同様である。

【0091】なお、本発明は、上述した実施の形態のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、その他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。また、暗号化の鍵情報に応じてデータを置換したり、転置したり、シフトレジスタ



を用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

#### 【0092】

【発明の効果】本発明に係るデータ記録方法によれば、入力デジタルデータを所定データ量単位でセクタ化するセクタ化工程と、ヘッダを付加するヘッダ付加工程と、誤り訂正符号化工程と、所定の変調方式で変調する変調工程と、同期パターンを付加する同期付加工程との、いずれか少なくとも1つの工程について、入力に対して暗号化処理を施して出力するようにしているため、どの工程で暗号化処理が施されたかも暗号の鍵となり、暗号の難易度を高くすることができる。これらの暗号化処理が施され得る工程の1つに、同一パターンを除去するためのランダム化処理を施すスクランブル処理工程を含めてもよい。また、既存の構成の一部を変更するだけで、簡単に暗号化が実現できるという利点もある。これらは、データ記録装置、記録媒体、再生方法及び装置の場合にも得られる効果である。

【0093】また、本発明によれば、誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施しているため、誤り訂正処理である程度データ復元が可能な状態から、データ復元が行えない状態までの任意のレベルの暗号化が行える。これによって、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、データ提供の用途に応じた、あるいはセキュリティレベルに応じた対応が可能となる。

【0094】また、誤り訂正処理の中で鍵のビット数の大きな暗号化が可能であり、誤り訂正符号化や復号化ICあるいはLSIのような巨大なブラックボックスの中で暗号化を実現しているため、一般ユーザによる解読を困難化し、データセキュリティを大幅に向上させることができる。

【0095】さらに、本発明によれば、所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部を、記録媒体のデータ記録領域とは別の領域に書き込んでおき、再生時にこの鍵情報の少なくとも一部の情報を読み取って、暗号復号化に用いる。暗号復号化の鍵情報が、記録媒体のデータ記録領域内の情報のみで完結しないため、暗号化の難易度が高まる。

【0096】またさらに、本発明によれば、データ列の同一パターンを除去するためのランダム化を主目的とするスクランブル処理の際に、生成多項式及び初期値の少なくとも一方を、暗号化の鍵に応じて変化させることにより、既存のスクランブル処理を暗号化に流用して、簡単な構成で暗号化を実現できる。

【0097】このようなデータの暗号化により、コピー防止や不正使用の防止が簡単な仕組みで実現でき、またセキュリティや課金システムへも容易に適用できる。

#### 【図面の簡単な説明】

【図1】本発明のデータ記録装置の第1の実施の形態の概略構成を示すブロック図である。

【図2】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック図である。

【図3】偶数・奇数バイトのインターリーブを説明するための図である。

【図4】スクランブラの一例を示す図である。

【図5】スクランブラのプリセット値の一例を示す図である。

【図6】生成多項式が可変のスクランブラの一例を示す図である。

【図7】セクタフォーマットの一例を示す図である。

【図8】セクタ内の同期領域での暗号化の一例を説明するための図である。

【図9】セクタ内のヘッダ領域の一例を示す図である。

【図10】誤り訂正符号化回路の一例の概略構成を示す図である。

【図11】誤り訂正符号化回路の一例の具体的な構成を示す図である。

【図12】誤り訂正符号化回路の他の例を示す図である。

【図13】変調回路での暗号化処理の一例を説明するための図である。

【図14】変調信号に付加される同期ワードの具体例を示す図である。

【図15】同期付加回路での暗号化の一例を説明するための図である。

【図16】データ記録媒体の一例を示す図である。

【図17】本発明のデータ再生装置の第1の実施の形態の概略構成を示すブロック図である。

【図18】復調回路での暗号化処理の一例を説明するための図である。

【図19】誤り訂正復号化回路の一例の概略構成を示す図である。

【図20】誤り訂正復号化回路の一例の具体的な構成を示す図である。

【図21】誤り訂正復号化回路の他の例を示す図である。

【図22】デスクランブル処理回路の一例を示す図である。

【図23】スクランブラの他の例を示す図である。

【図24】図23のスクランブラのプリセット値の一例を示す図である。

【図25】セクタフォーマットの他の例を示す図である。

【図26】図25のセクタフォーマットにおけるセクタ内のヘッダ領域の一例を示す図である。

【図27】誤り訂正符号化回路の他の例を示すブロック図である。

【図28】誤り訂正符号の具体例としての積符号を示す図である。

【図29】セクタの信号フォーマットの一例を示す図である。

【図30】変調信号に付加される同期ワードの他の具体例を示す図である。

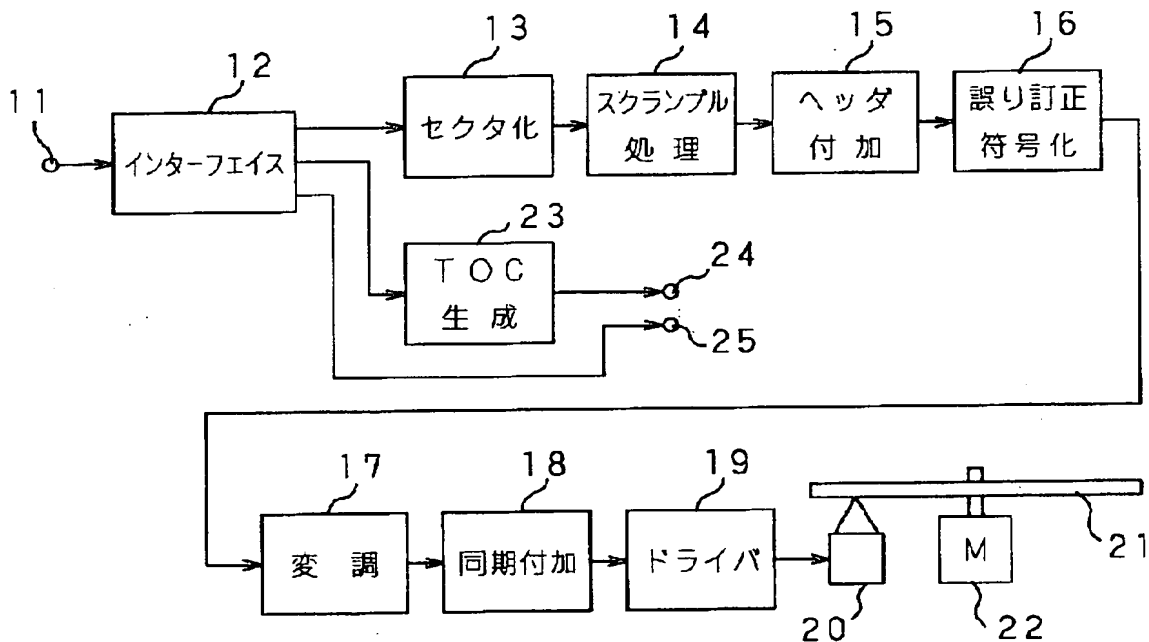
【図31】同期付加回路での暗号化の他の例を説明するための図である。

【図32】誤り訂正復号化回路の他の例を示すブロック図である。

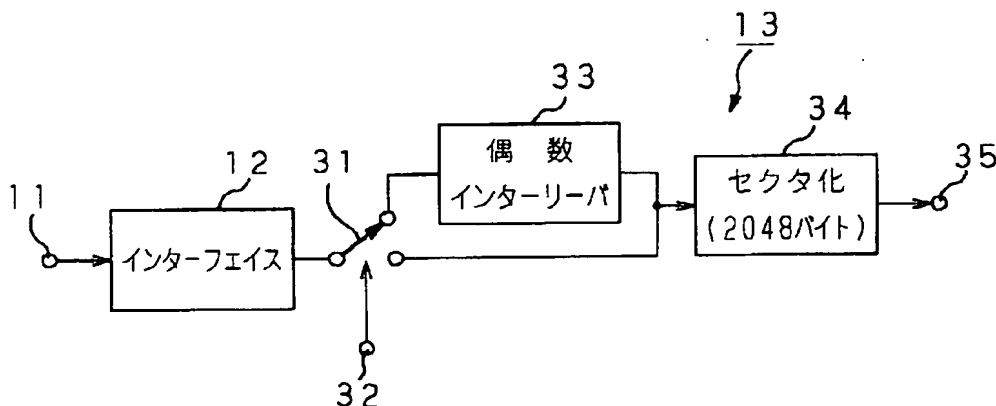
【符号の説明】

13 セクタ化回路、14 スクランブル処理回路、15 ヘッダ付加回路、16 誤り訂正符号化回路、17 変調回路、18 同期付加回路、57、142 再配列回路、61、66、151、156 ExOR回路群、114 同期分離回路、115 復調回路、116 誤り訂正復号化回路、117 セクタ分解回路、118 ヘッダ分離回路、119 デスクランブル処理回路

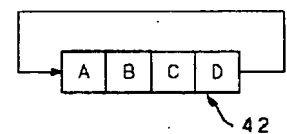
【図1】



【図2】



【図8】





【図 7】

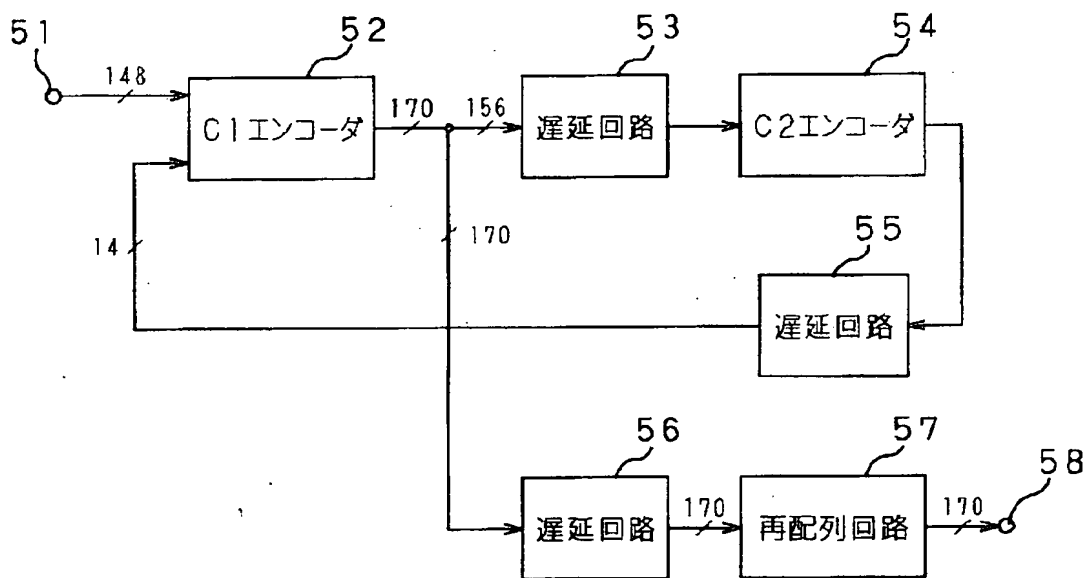
位置	+0	+1	+2	+3	サイズ
0	同期				4
4	ヘッダ				16
20	ユーザデータ				2048
2068	誤り検出符号 ( EDC )				46

サイズ合計: 2072バイト

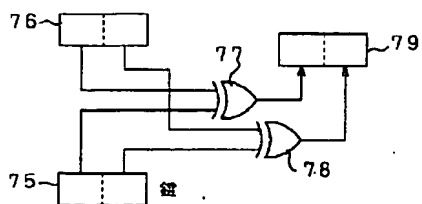
【図 14】

符号ワード	符号ワード					
	msb	同期パターン a	lsb	msb	同期パターン b	lsb
S0	00010010010000000000100000000001		10010010010000000000100000000001			
S1	00010000010000000000100000000001		10010000010000000000100000000001			
S2	00000100010000000000100000000001		10000100010000000000100000000001			
S3	00001000010000000000100000000001		10001000010000000000100000000001			

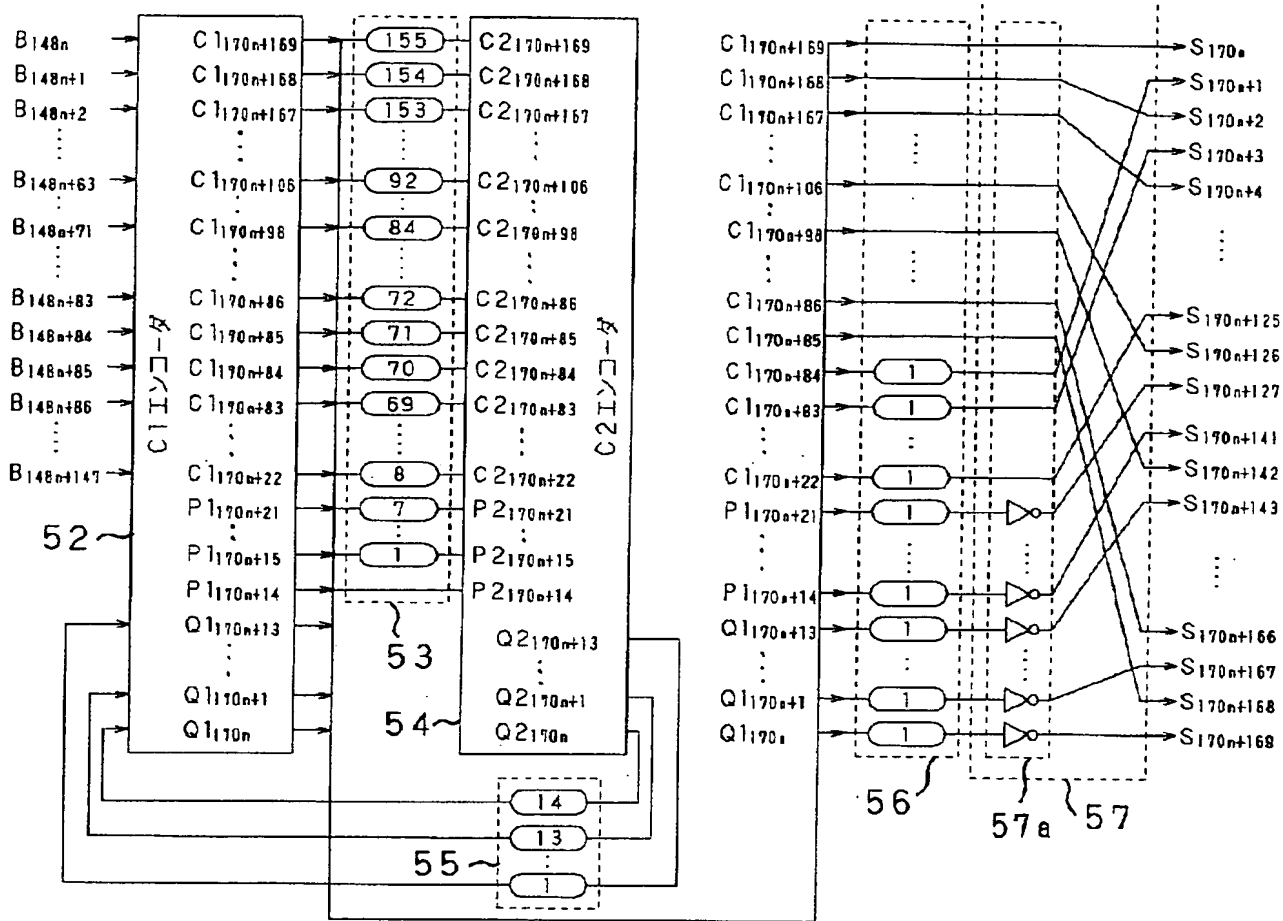
【図 10】



【図 15】

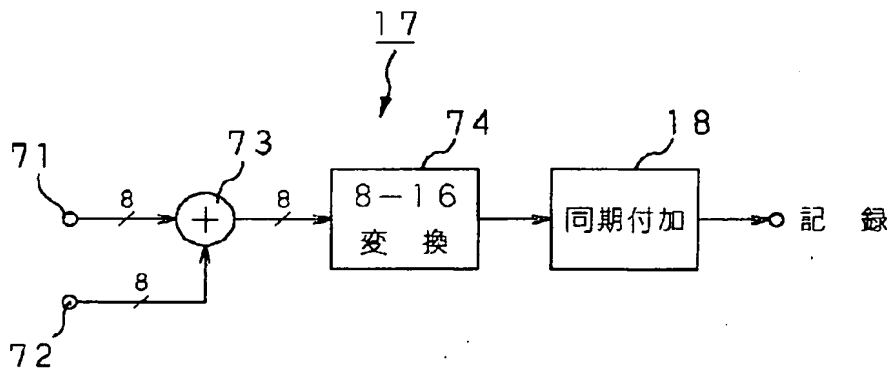


【図 11】



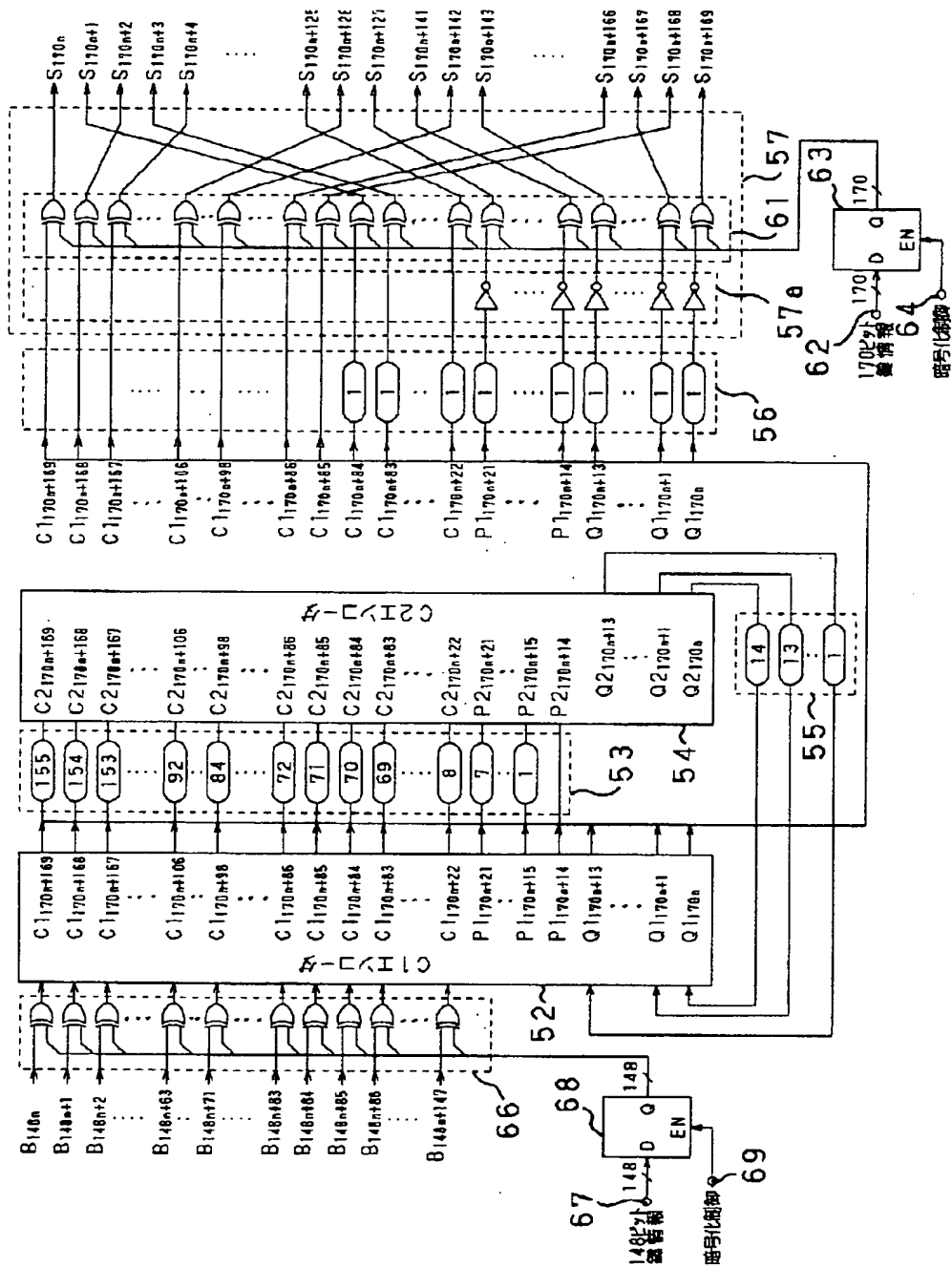
【図 13】

【図 24】

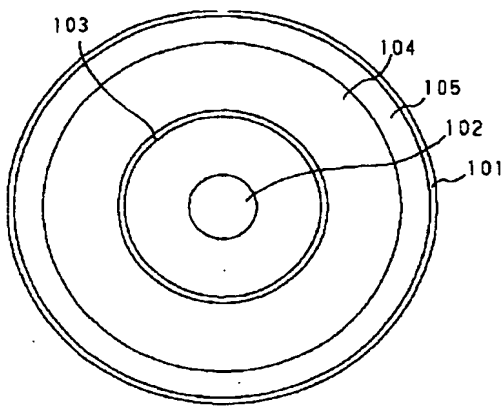


選択番号	プリセット値	選択番号	プリセット値
0	\$0001	8	\$0010
1	\$5500	9	\$5000
2	\$0002	10	\$0020
3	\$2A00	11	\$2001
4	\$0004	12	\$0040
5	\$5400	13	\$4002
6	\$0008	14	\$0080
7	\$2800	15	\$0005

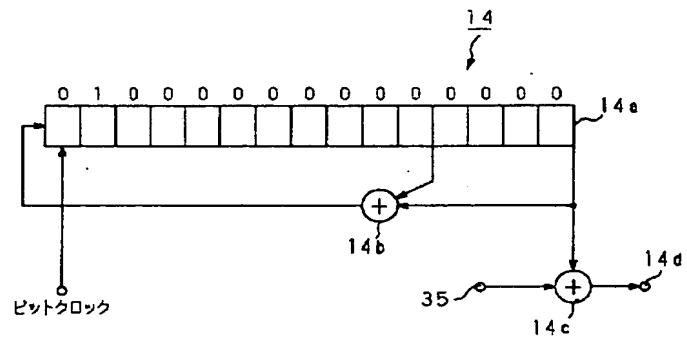
【図12】



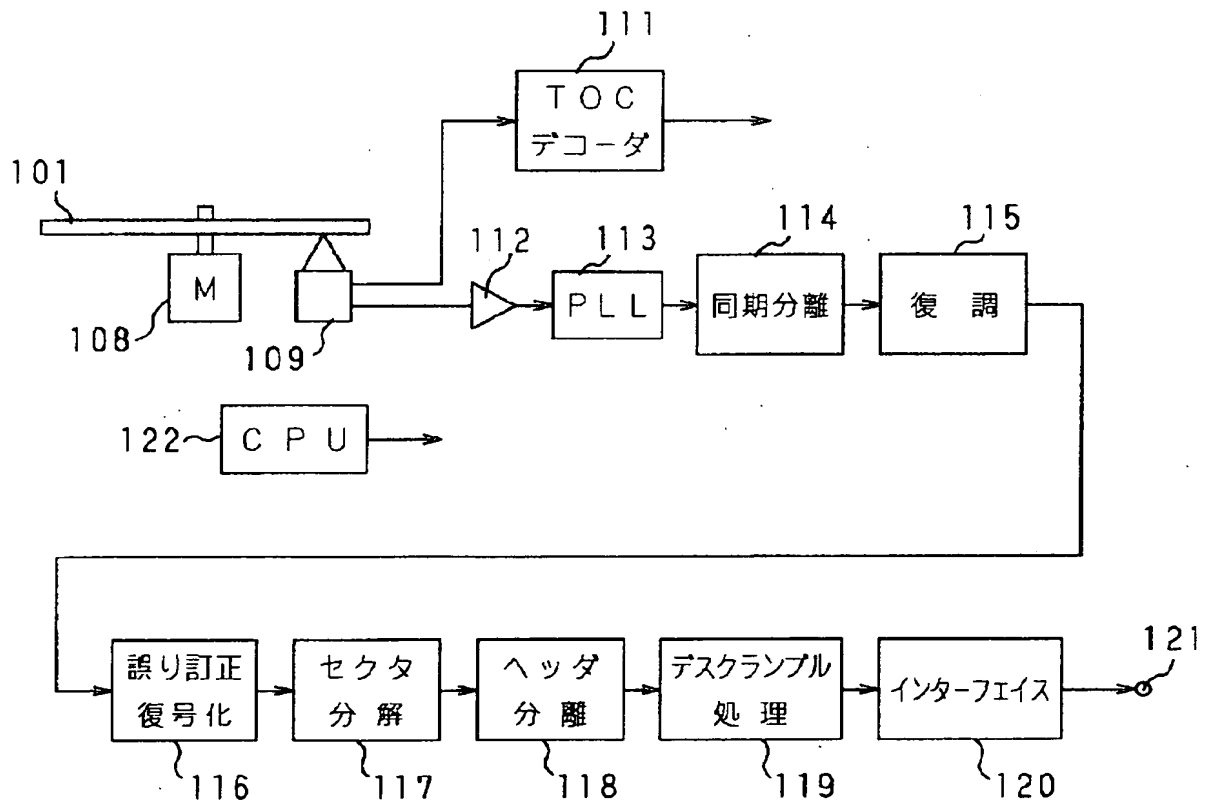
【図 16】



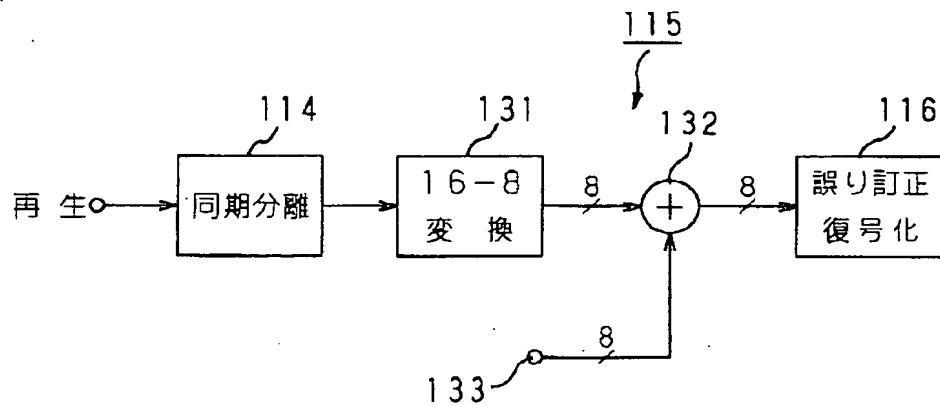
【図 23】



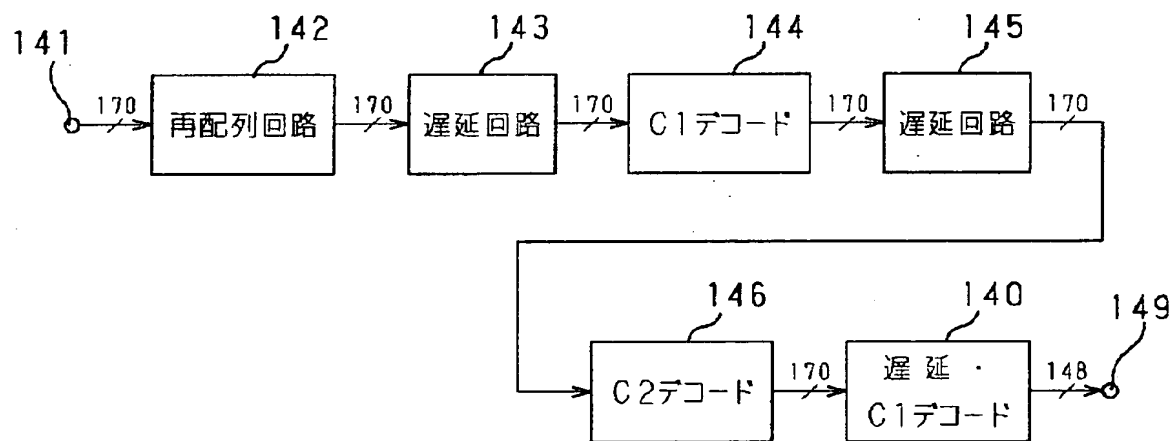
【図 17】



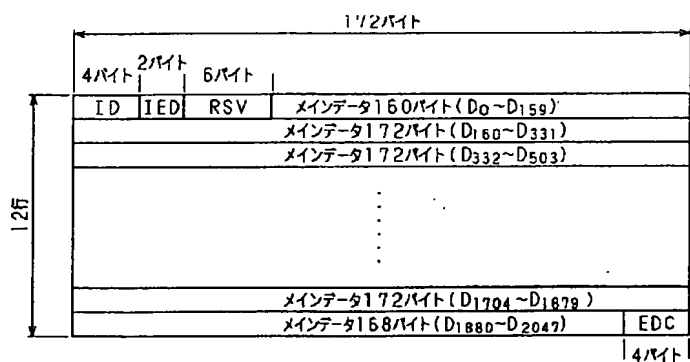
【図18】



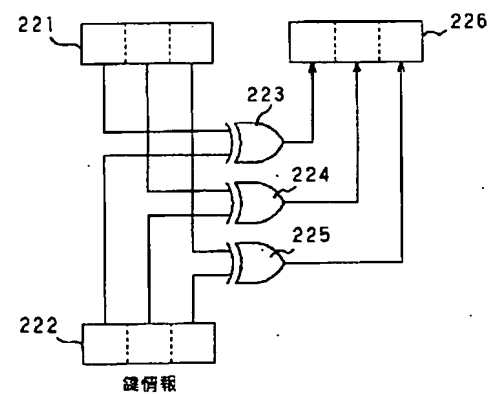
【図19】



【図25】

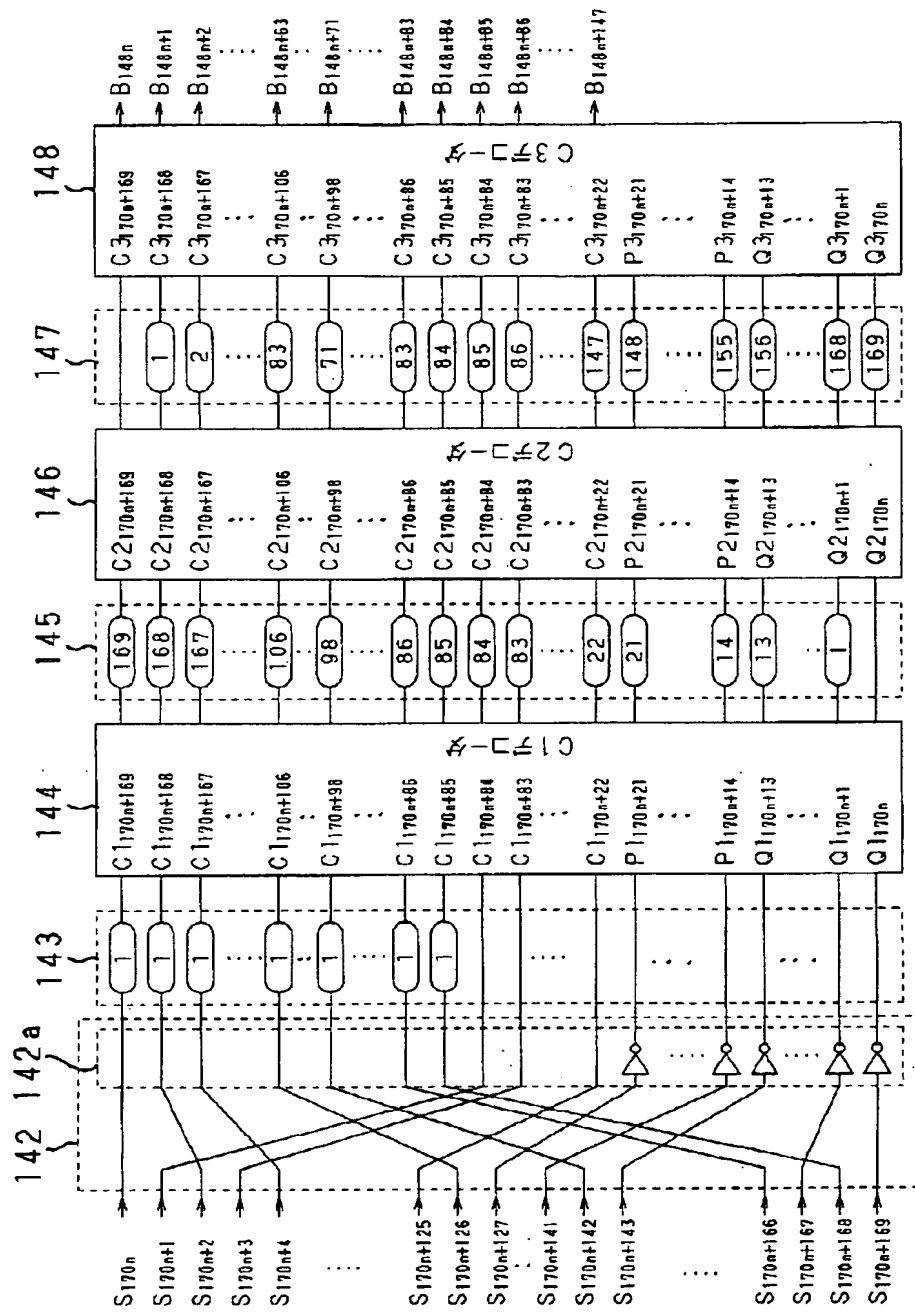


【図31】

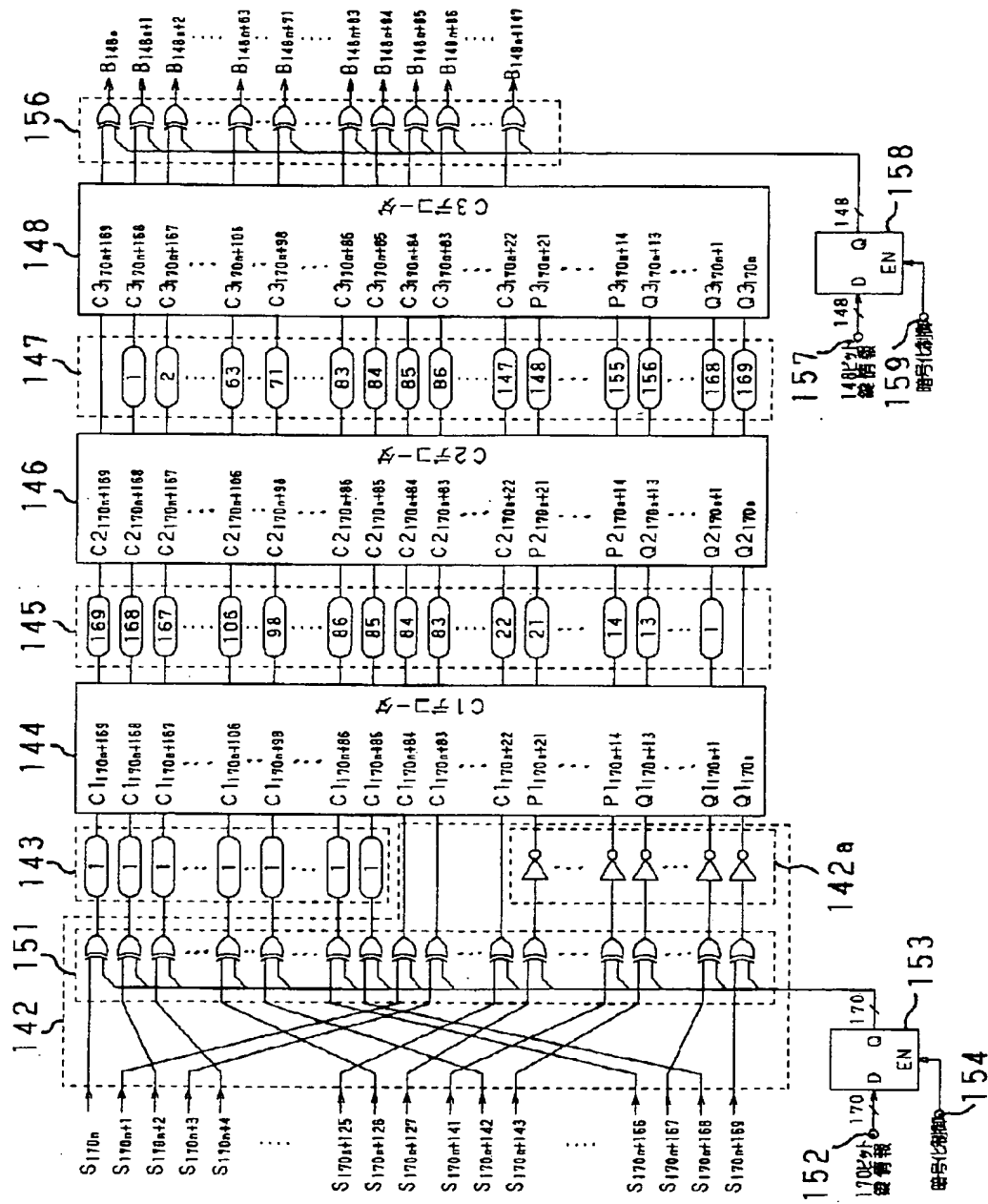




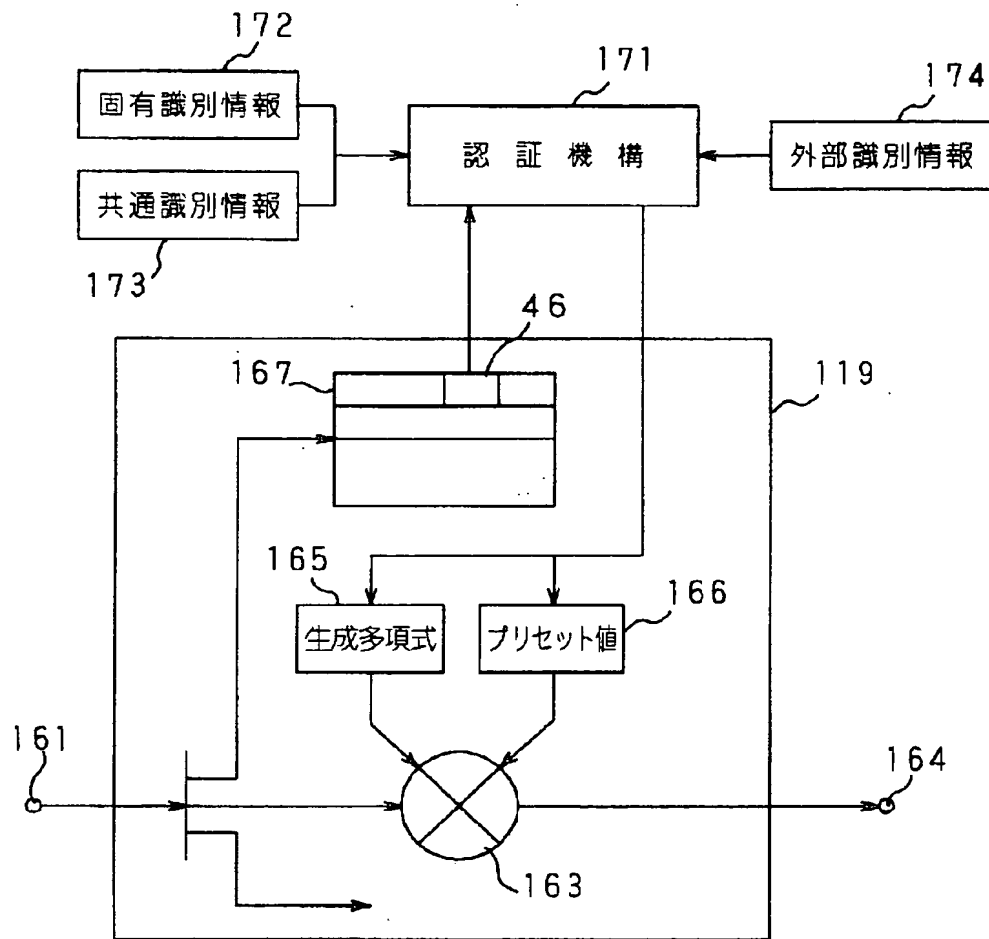
【図20】



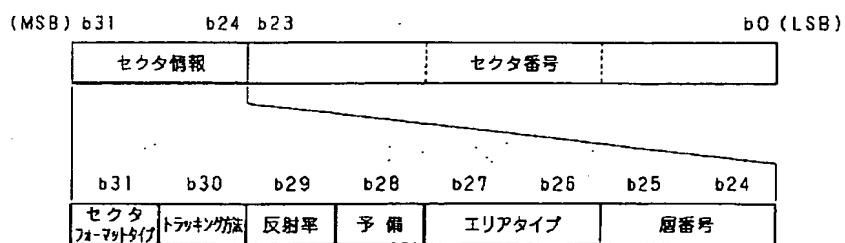
【図21】



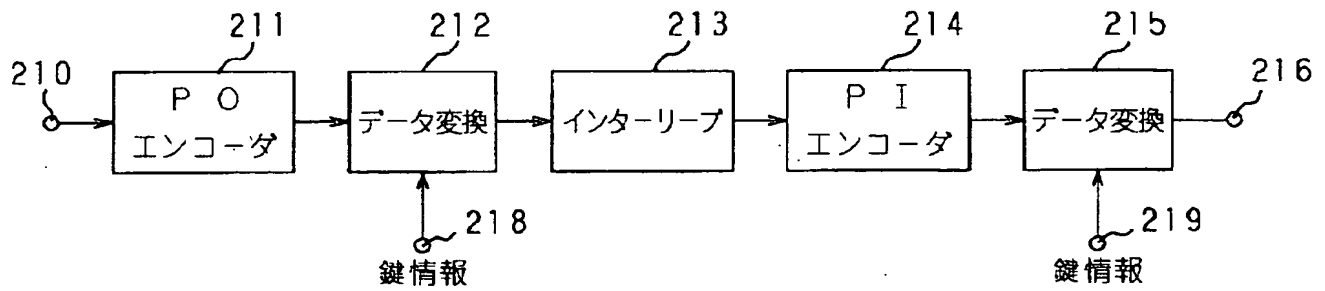
【図 2 2】



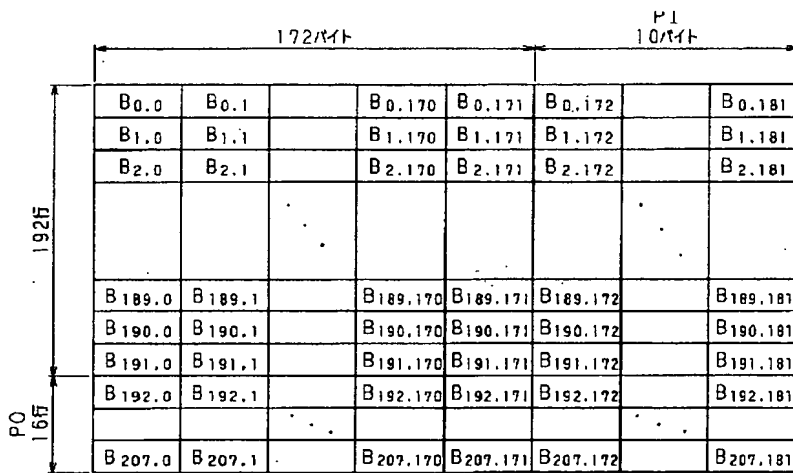
【図 2 6】



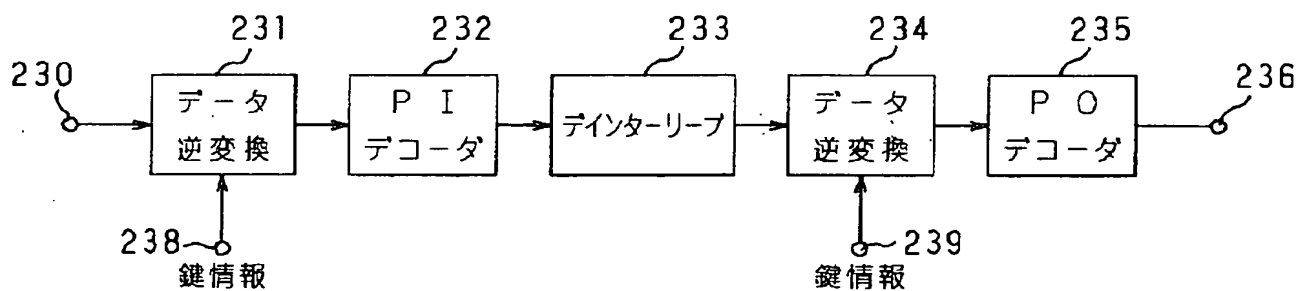
【図27】



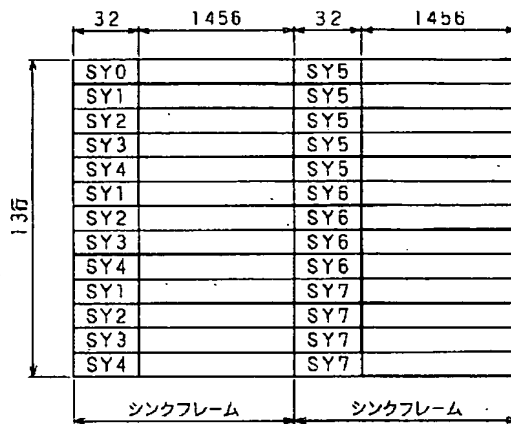
【図28】



【図32】



【図29】



【図30】

(a) ステート1及び2

(MSB)	(LSB)	(MSB)	(LSB)
SY0=0001001001000100	0000000000010001	/	0001001000000100 0000000000010001
SY1=0000010000000100	0000000000010001	/	0000010001000100 0000000000010001
SY2=0001000000000100	0000000000010001	/	0001000001000100 0000000000010001
SY3=0000100000000100	0000000000010001	/	0000100001000100 0000000000010001
SY4=0010000000000100	0000000000010001	/	0010000001000100 0000000000010001
SY5=0010001001000100	0000000000010001	/	0010001000000100 0000000000010001
SY6=0010010010000100	0000000000010001	/	0010000100000100 0000000000010001
SY7=0010010001000100	0000000000010001	/	0010010000000100 0000000000010001

(b) ステート3及び4

(MSB)	(LSB)	(MSB)	(LSB)
SY0=1001001000000100	0000000000010001	/	1001001001000100 0000000000010001
SY1=1000010001000100	0000000000010001	/	1000010000000100 0000000000010001
SY2=1001000001000100	0000000000010001	/	1001000000000100 0000000000010001
SY3=1000001001000100	0000000000010001	/	1000001000000100 0000000000010001
SY4=1000100001000100	0000000000010001	/	1000100000000100 0000000000010001
SY5=1000100100000100	0000000000010001	/	1000001000000100 0000000000010001
SY6=1001000010000100	0000000000010001	/	1000000010000100 0000000000010001
SY7=1000100010000100	0000000000010001	/	1000000010000100 0000000000010001

【手続補正書】

【提出日】平成8年7月19日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】図面の簡単な説明

【補正方法】変更

【補正内容】

【図面の簡単な説明】

【図1】本発明のデータ記録装置の第1の実施の形態の

概略構成を示すブロック図である。

【図2】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック図である。

【図3】偶数・奇数バイトのインターリーブを説明するための図である。

【図4】スクランブラの一例を示す図である。

【図5】スクランブラのプリセット値の一例を示す図で

ある。

【図 6】生成多項式が可変のスクランブラの一例を示す図である。

【図 7】セクタフォーマットの一例を示す図である。

【図 8】セクタ内の同期領域での暗号化の一例を説明するための図である。

【図 9】セクタ内のヘッダ領域の一例を示す図である。

【図 10】誤り訂正符号化回路の一例の概略構成を示す図である。

【図 11】誤り訂正符号化回路の一例の具体的な構成を示す図である。

【図 12】誤り訂正符号化回路の他の例を示す図である。

【図 13】変調回路での暗号化処理の一例を説明するための図である。

【図 14】変調信号に付加される同期ワードの具体例を示す図である。

【図 15】同期付加回路での暗号化の一例を説明するための図である。

【図 16】データ記録媒体の一例を示す図である。

【図 17】本発明のデータ再生装置の第 1 の実施の形態の概略構成を示すブロック図である。

【図 18】復調回路での暗号化処理の一例を説明するための図である。

【図 19】誤り訂正復号化回路の一例の概略構成を示す図である。

【図 20】誤り訂正復号化回路の一例の具体的な構成を示す図である。

【図 21】誤り訂正復号化回路の他の例を示す図である。

【図 22】デスクランブル処理回路の一例を示す図である。

【図 23】スクランブラの他の例を示す図である。

【図 24】図 23 のスクランブラのプリセット値の一例を示す図である。

【図 25】セクタフォーマットの他の例を示す図である。

【図 26】図 25 のセクタフォーマットにおけるセクタ内のヘッダ領域の一例を示す図である。

【図 27】誤り訂正符号化回路の他の例を示すブロック図である。

【図 28】誤り訂正符号の具体例としての積符号を示す図である。

【図 29】セクタの信号フォーマットの一例を示す図である。

【図 30】変調信号に付加される同期ワードの他の具体例を示す図である。

【図 31】同期付加回路での暗号化の他の例を説明するための図である。

【図 32】誤り訂正復号化回路の他の例を示すブロック図である。

【符号の説明】

13 セクタ化回路、 14 スクランブル処理回路、  
15 ヘッダ付加回路、 16 誤り訂正符号化回路、  
17 変調回路、 18 同期付加回路、 57、  
142 再配列回路、 61、66、151、156  
ExOR回路群、114 同期分離回路、 115 復調回路、  
116 誤り訂正復号化回路、117 セクタ分解回路、  
118 ヘッダ分離回路、 119 デスクランブル処理回路

フロントページの続き

(72)発明者 大澤 義知  
東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内

(72)発明者 応和 英男  
東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 6 部門第 3 区分

【発行日】平成 14 年 2 月 28 日 (2002. 2. 28)

【公開番号】特開平 9-73414

【公開日】平成 9 年 3 月 18 日 (1997. 3. 18)

【年通号数】公開特許公報 9-735

【出願番号】特願平 8-98949

【国際特許分類第 7 版】

G06F 12/14 320

G09C 1/00 660

G11B 20/10

20/12 102

20/18 570

【F I】

G06F 12/14 320 B

G09C 1/00 660 D

G11B 20/10 H

20/12 102

20/18 570 N

【手続補正書】

【提出日】平成 13 年 7 月 19 日 (2001. 7. 19)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】0026

【補正方法】変更

【補正内容】

【0026】先ず、セクタ化回路 13 においては、例えば図 2 に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図 2 において、上記図 1 のインターフェース回路 12 からの出力を、2 出力の切換スイッチ 31 に送り、この切換スイッチ 31 の一方の出力を偶奇インターリーバ 33 を介してセクタ化器 34 に送り、切換スイッチ 31 の他方の出力をそのままセクタ化器 34 に送っている。セクタ化器 34 では、例えば入力データの 2048 バイト単位でまとめて 1 セクタとしている。このセクタ化回路 13 の切換スイッチ 31 の切換動作を、鍵となる 1 ビットの制御信

号で制御するわけである。偶奇インターリーバ 33 は、図 3 の A に示すような偶数バイト 36a と奇数バイト 36b とが交互に配置された入力データの 1 セクタ分を、図 3 の B に示すように、偶数データ部 37a と奇数データ部 37b とに分配して出力する。さらに、図 3 の C に示すように、1 セクタ内の所定の領域 39 を鍵情報により特定し、この領域 39 内のデータについてのみ偶数データ部 39a と奇数データ部 39b とに分配するようにしてもよい。この場合には、領域 39 の特定の仕方を複数通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。

【手続補正 2】

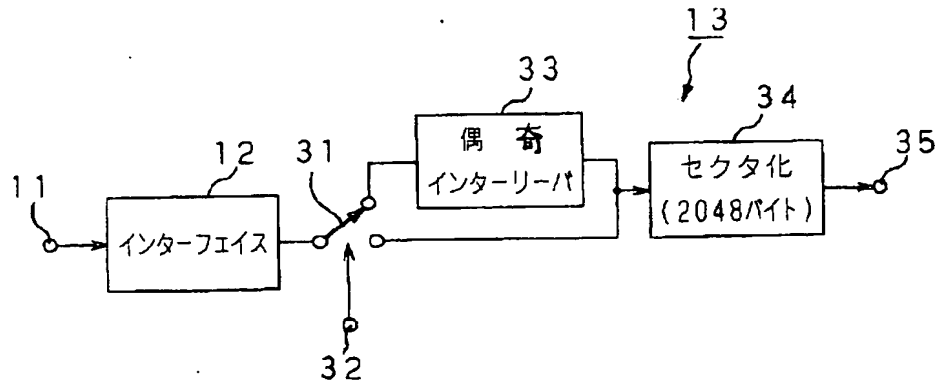
【補正対象書類名】図面

【補正対象項目名】図 2

【補正方法】変更

【補正内容】

【図 2】



【手続補正 3】

【補正対象書類名】図面

【補正対象項目名】図 6

【補正方法】変更

【補正内容】

【図 6】

